Après l'installation de base de Debian 12 :

Aller dans /etc/network et modifier le fichier interfaces.

Modifier le réseau par défaut en static
puis renseigner l'**ip**, le **masque**, la **passerelle**
et le **dns**.

Ensuite aller dans /etc/ssh et modifier le fichier sshd_config.

Aller à la ligne permit root login, décommenter la
Et remplacé **prohibitpassword** par **yes**.

Si ssh n'est pas installer redémarrer le serveur.

Ensuite installer ssh : **apt install ssh.**

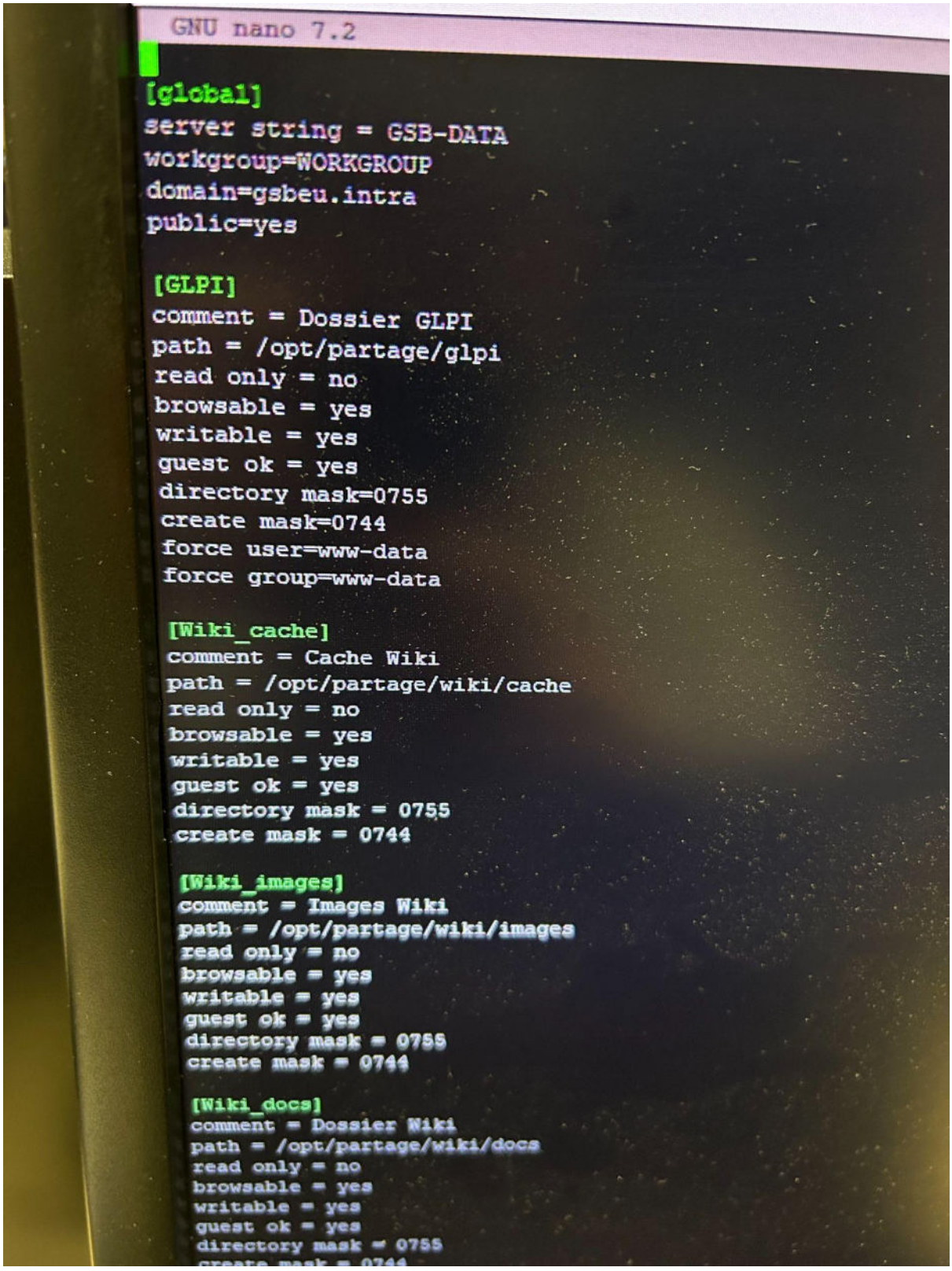
PARTAGE SAMBA

Pour faire un partage samba il faut déjà l'installer.
Pour cela taper la commande : apt install samba
Ensuite créer votre partage : (pour des soucis de simplicité on utilisera uniquement les guest)

[global]
server string = GSB-DATA (Nom du Serveur)
workgroup = WORKGROUP (dans le cas ou on voudrait connecter une machine windows hors domaine)
domain = gsbeu.intra (domaine du serveur)
public = yes

[NomDuPartage]
comment = commentaireutile.txt
path = /opt/partage/glpi (chemin du partage sur la machine samba)
read only = no (déclare si le dossier est en lecture seul)
browsable = yes (déclare si l'utilisateur peut traverser le dossier)
writable = yes (déclare si l'utilisateur peut écrire sur le dossier)
directory mask = 0755 (choisi les droits pour les utilisateurs, les groupes pour le dossier)
create mask = 0744 (choisi les droits pour les utilisateurs, les groupes pour les fichiers)
force user = Nom_Ut (change le propriétaire par l'utilisateurs désigné)
force group = Nom_Grp (change le groupe propriétaire par le groupe désigné)

Exemple pris du contexte :


GNU nano 7.2
[global]
server string = GSB-DATA
workgroup=WORKGROUP
domain=gsbeu.intra
public=yes
[GLPI]
comment = Dossier GLPI
path = /opt/partage/glpi
read only = no
browsable = yes
writable = yes
guest ok = yes
directory mask=0755
create mask=0744
force user=www-data
force group=www-data
[Wiki_cache]
comment = Cache Wiki
path = /opt/partage/wiki/cache
read only = no
browsable = yes
writable = yes
guest ok = yes
directory mask = 0755
create mask = 0744
[Wiki_images]
comment = Images Wiki
path = /opt/partage/wiki/images
read only = no
browsable = yes
writable = yes
guest ok = yes
directory mask = 0755
create mask = 0744
[Wiki_docs]
comment = Dossier Wiki
path = /opt/partage/wiki/docs
read only = no
browsable = yes
writable = yes
guest ok = yes
directory mask = 0755

LOAD BALANCER

URL : IP de l'une des machines du load balancer
Y : Port associé à l'ip du serveur
Proto : Protocole utilisé (http ou ws)
/ : Chemin d'accès par défaut (/images si il faut accéder qu'à images)
Prefix.Domain.Suffix : Adresse taper dans la barre de recherche par l'utilisateur
m : Méthode de LoadBalancing (byrequests ou bytraffic) à choisir en fonction de besoin
port lb : Port côté load balancer exposé à l'utilisateur
Balancer : Toto Nom du LoadBalancer

Parti Mémo :
URL:Y
Proto://URL:Y
"/" prefix.domain.suffix Taper par l'ut
/ = route par défaut, préciser un dossier pour n'afficher que ce dernier
Method Loadbalancing : m Requests/Traffic

```
<VirtualHost *:ports lb>
        ServerName prefix.domain.suffix
        <Proxy Balancer ://Toto>
                Balancer Member proto://URL:Y          Autant qu'il y a de
LB
                Proxy Set lbmethod = m
                        Proxy Set stickysession = routeid          Nécessaire
        pour garder session                                        d'un
        serv à l'autre
        </Proxy>
        Proxy Pass "/" "balancer://Toto"
        Proxy Pass Reverse "/" "balancer://Toto"
</VirtualHost>
```

INFO CONTEXTE :
IP BDD : 10.10.3.210 ID : 70
IP LB : 172.16.0.20 ID : 80

Mise en place de la VIP entre les serveurs :

sur tous les noeuds :

apt install keepalived

nano /etc/keepalived/keepalived.conf

```
# Paramètres généraux
global_defs {
   enable_script_security
}

# Programme_X est-il en cours d'exécution ?
vrrp_script check_Programme_X {    A remplacer par le programme que l'on garder ouvert
   script "/usr/bin/pgrep Programme_X"
   interval 1
   fall 2
   rise 2
}

# Configuration interface virtuelle
vrrp_instance VIP {
   interface ens19 (ou nom de l'interface exposée)
   state MASTER
   priority 100
   virtual_router_id 70
   authentication {
      auth_type PASS
      auth_pass MONSUPERPASSWORD (MAX 8 caractères)
   }
   virtual_ipaddress {
      XX.XX.XX.XX (ip à partager)
   }
   track_script {
      check_Programme_X
   }
}
```

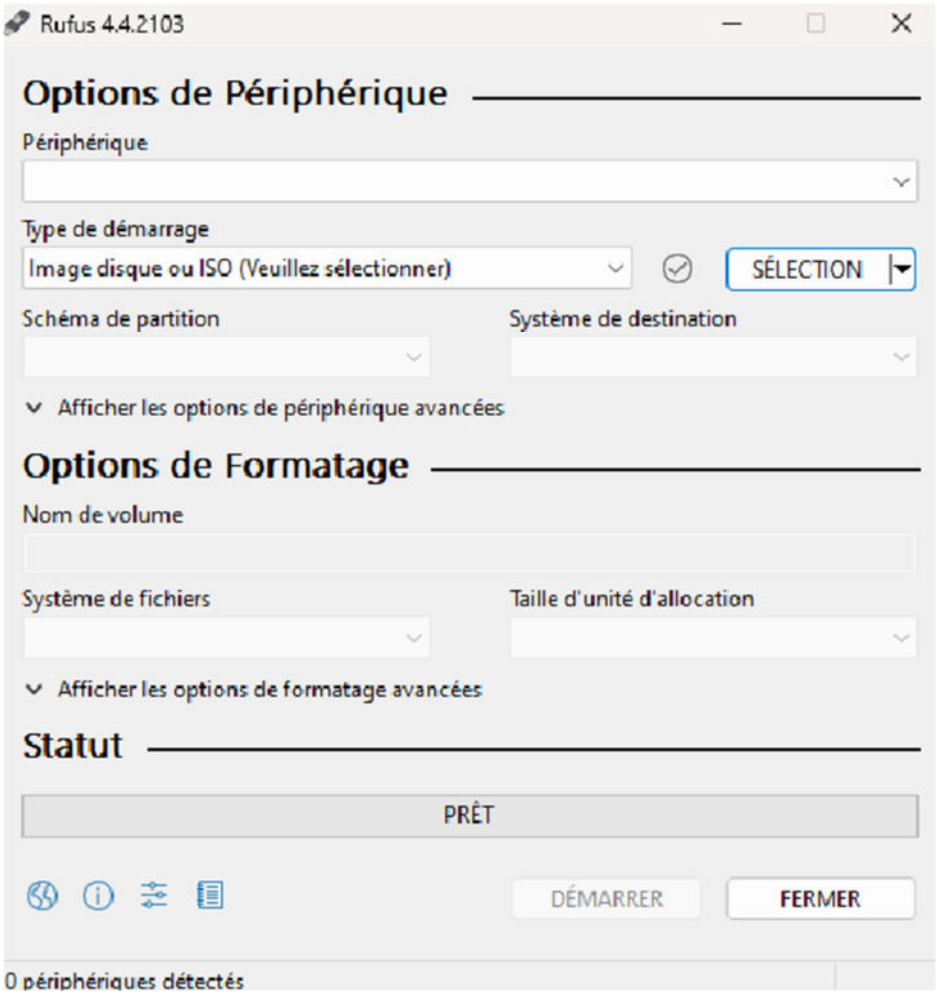
On veillera à avoir le même virtual_router_id entre les machines SQL.
La priorité doit être différente entre tous les serveurs (entre 1 et 255, 255 étant le plus prioritaire) par exemple :

- Master : 150
- Slave 1 : 100
- Slave 2 : 90
- Slave 3 : 80

chmod 600 /etc/keepalived/keepalived.conf
useradd -U -M -s /sbin/nologin keepalived_script
systemctl restart keepalived
systemctl status keepalived

Installation d'un proxy PFSENSE :

Etape 1 : créer une clé bootable avec l'iso PFSENSE via l'utilitaire rufus



Etape 2 : lancer l'installation sur le serveur

Etape 3 : configurer nos deux interfaces réseaux

Nous choisirons **l'interface r10 pour notre interface WAN** (celle qui est tournée vers la sortie de notre switch cisco)

Nous choisirons **l'interface bge0 qui sera notre interface LAN** (vers notre borne wifi)

Nous allons faire une détection automatique pour chaque interface :

Taper a (pour la détection automatique), lorsque la détection se lance, connecter le câble réseau à l'interface souhaitée.

Dès lors que le statut de l'interface affiche (link state changed to up) et que le port du switch est remonté, appuyer sur entrée.

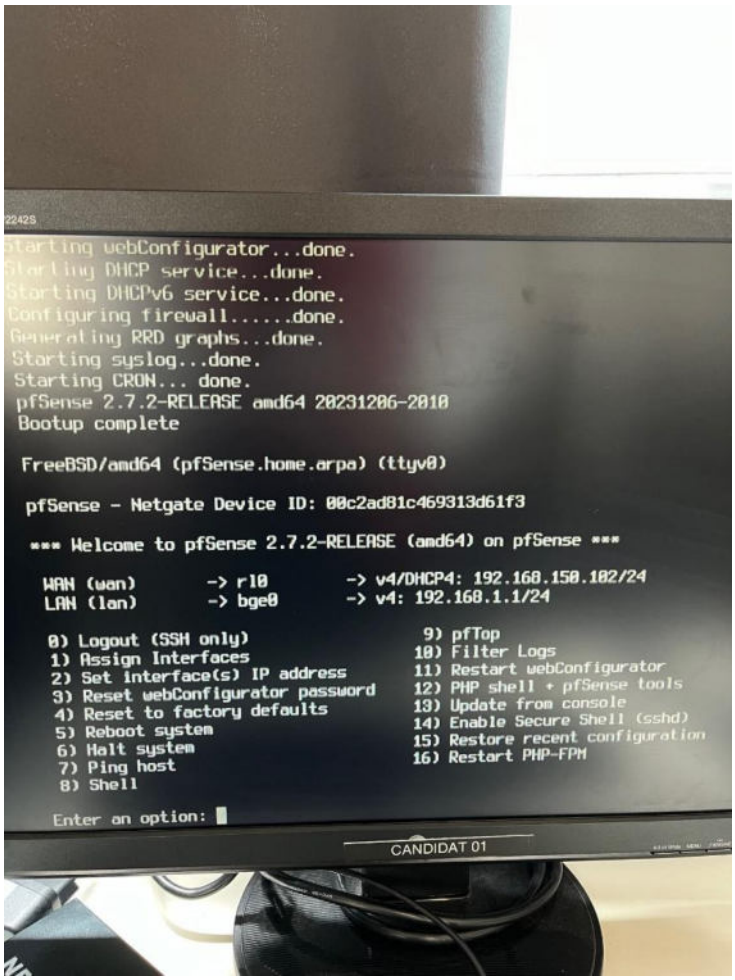
Notre première interface est alors détectée

Ensuite, appuyer sur la touche a (pour la détection automatique), lorsque la détection se lance, connecter le câble réseau à l'interface souhaitée.

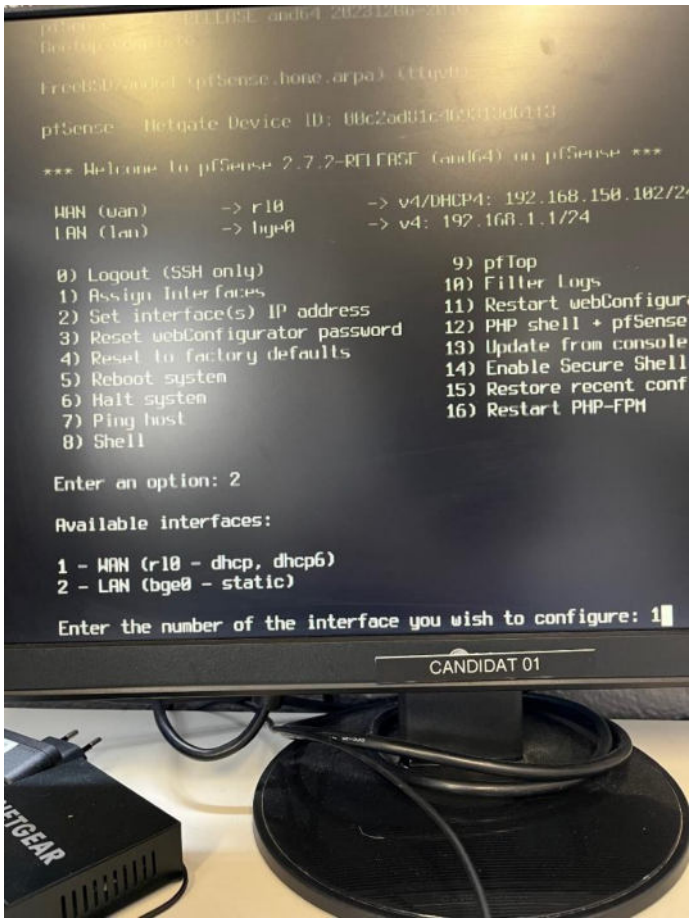
Dès lors que le statut de l'interface affiche (link state changed to up) et que le port de la borne wifi est remonté, appuyer sur entrée.

Etape 4 : affecter les adresses IP aux interfaces

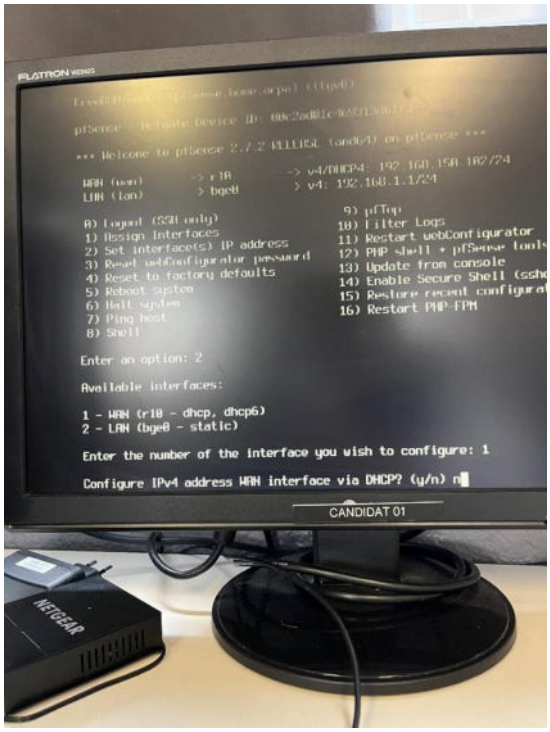
Choisir « set interface IP address » en appuyant sur la touche 2 puis sélectionner notre interface (nous commencerons par r10)



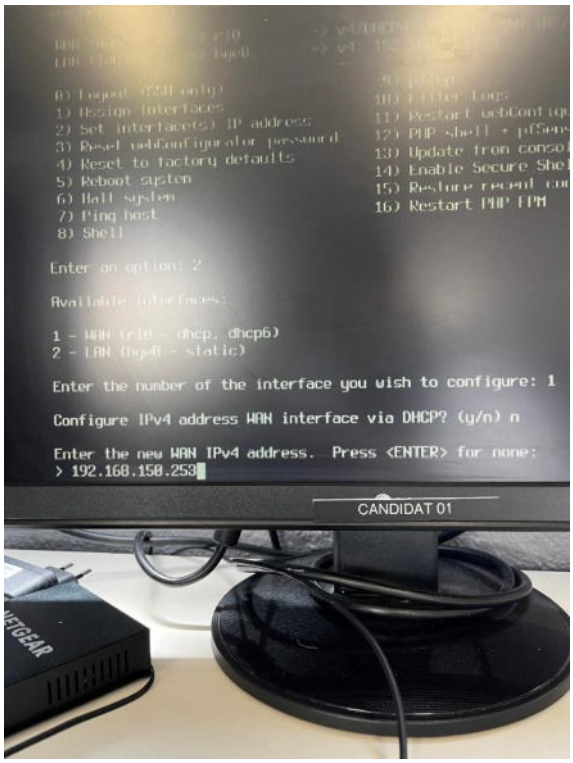
Nous choisirons tout d’abord l’interface r10



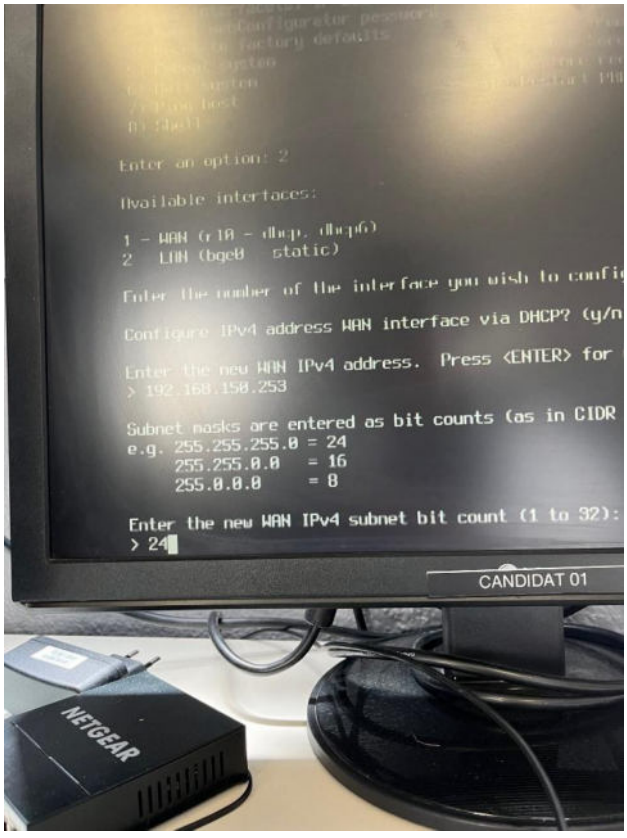
Ne pas configurer l’ip en DHCP



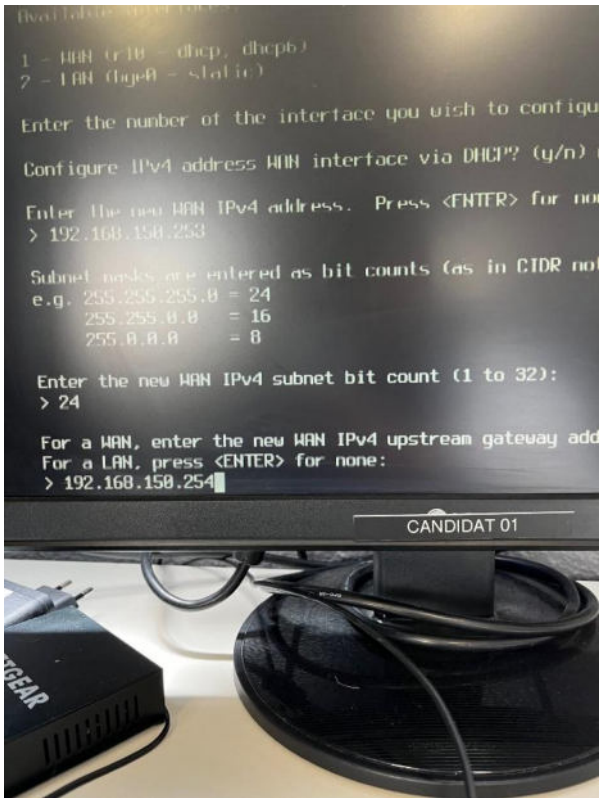
Entrer l’adresse IP

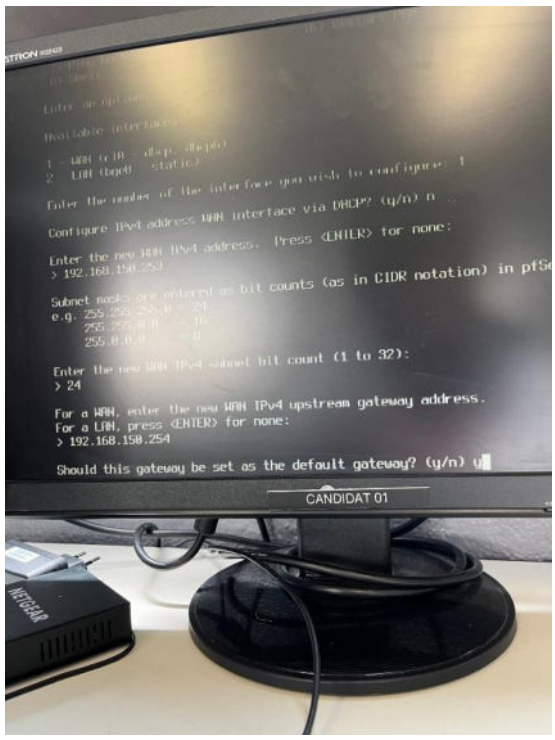


Entrer son masque

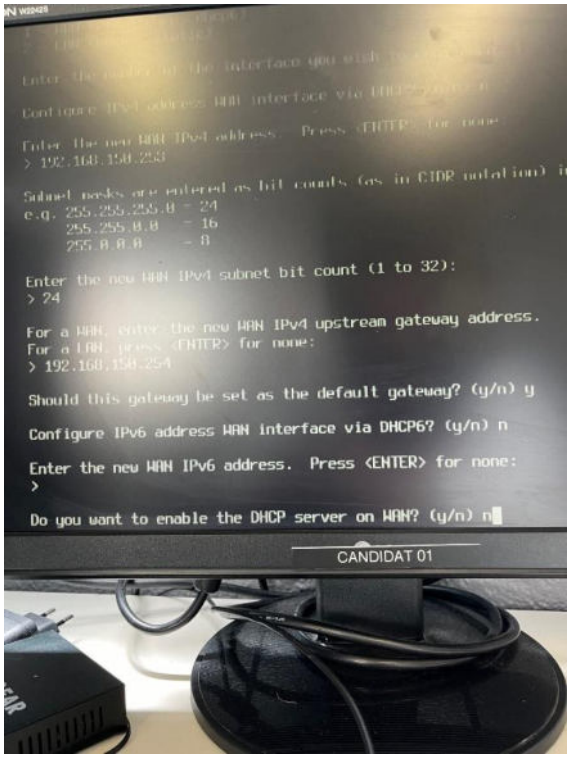


Indiquer la passerelle (nœud de niveau 3 le plus proche de notre interface wan qui est la passerelle du réseau 150 du switch cisco) et la mettre en défaut

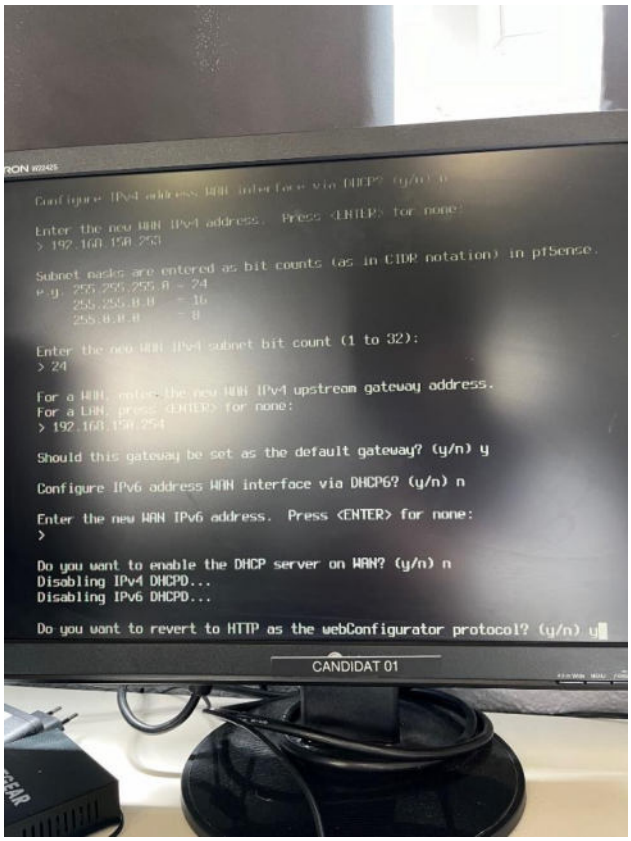




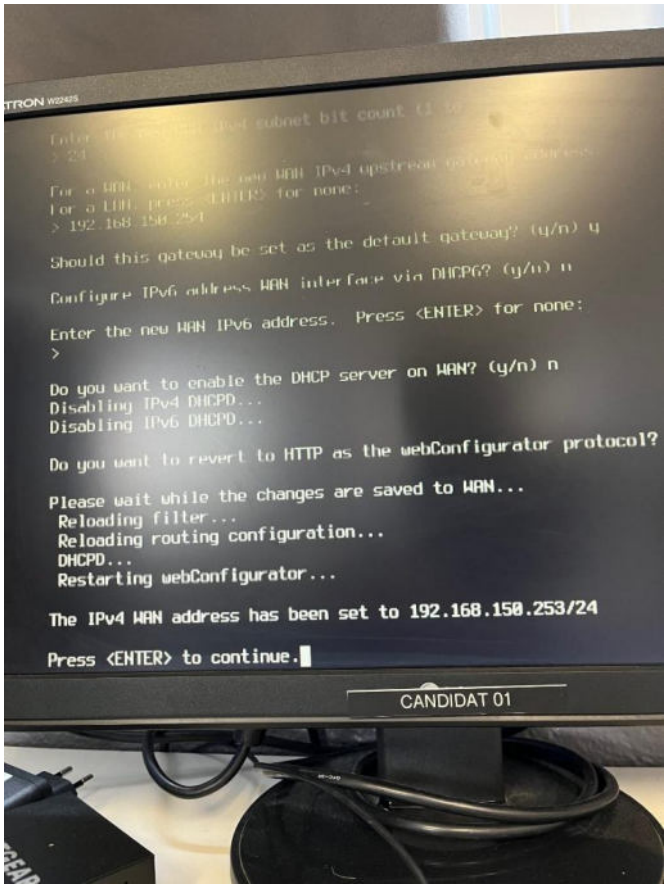
Nous ne configurerons pas d'IPV6 via DHCPV6 ni d'IPV6 en statique puis désactiver le DHCP



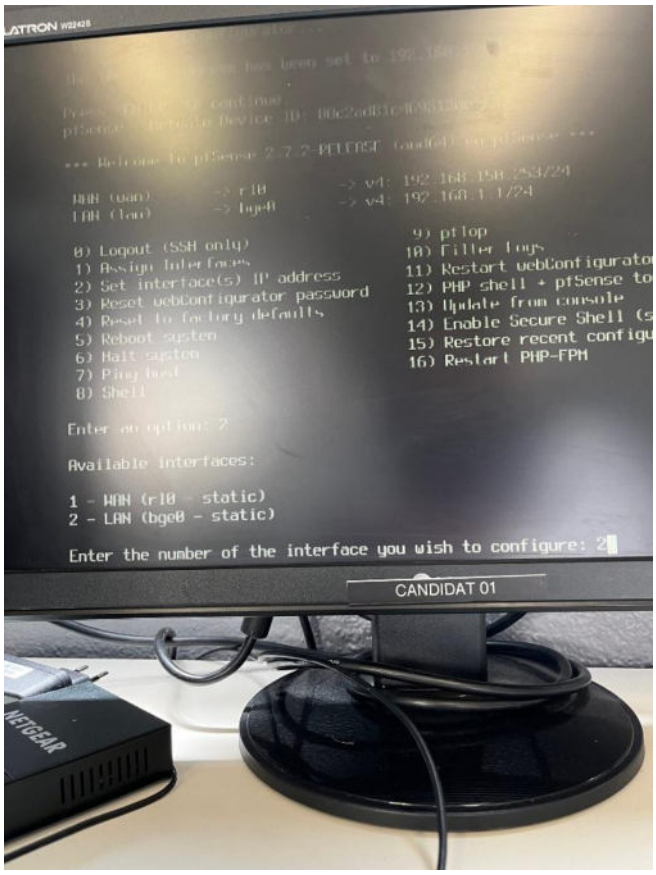
Nous laisserons le protocole web http par défaut



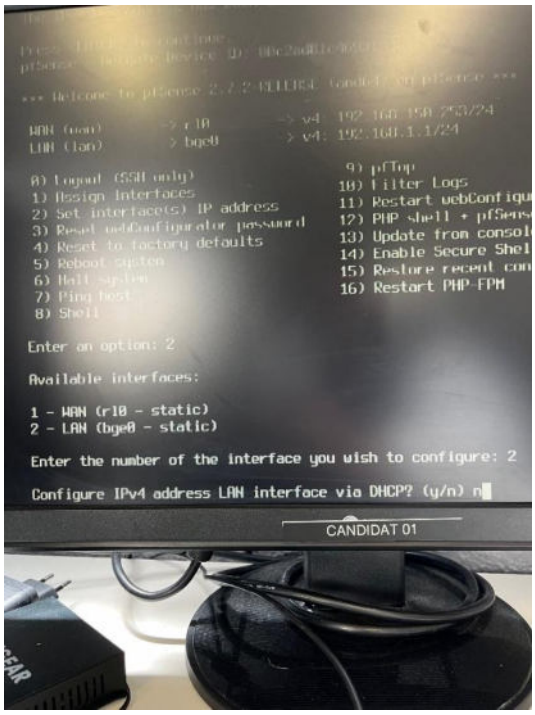
L’interface r10 est alors configurée



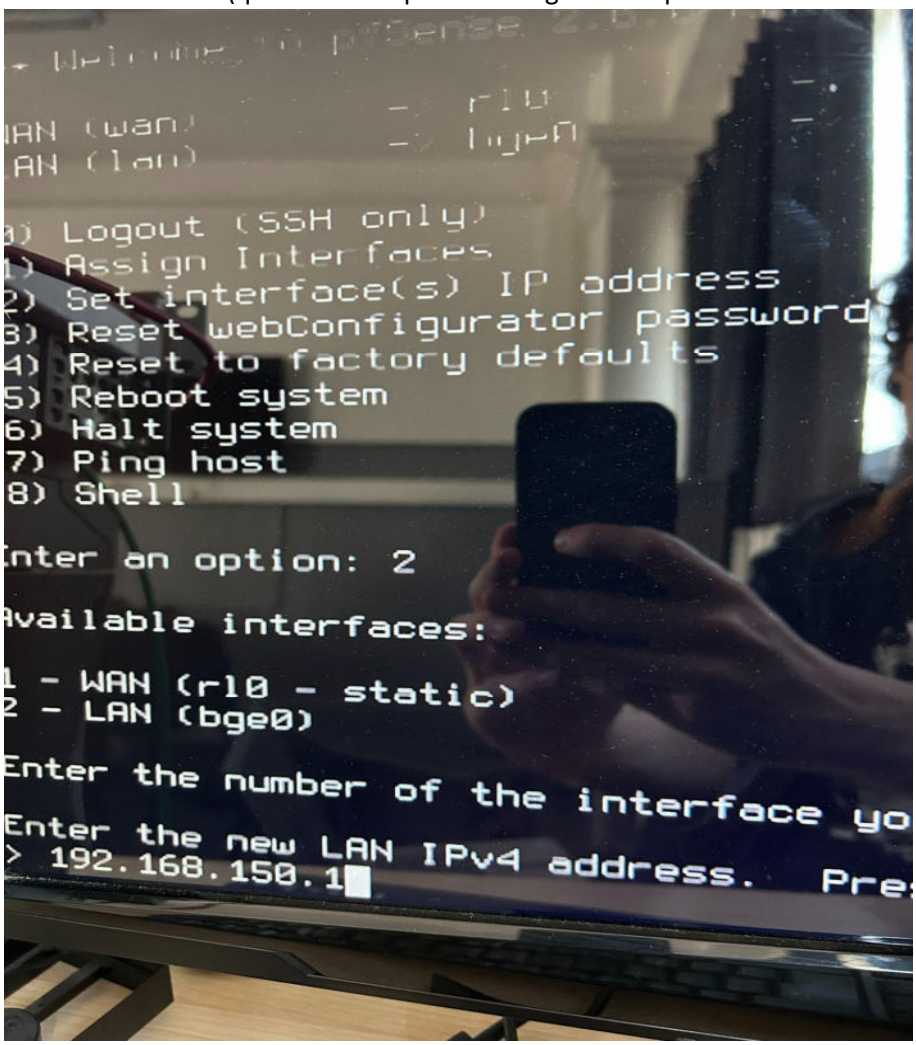
Pour l'interface bge0, Choisir « set interface IP address » puis sélectionner notre interface bge0



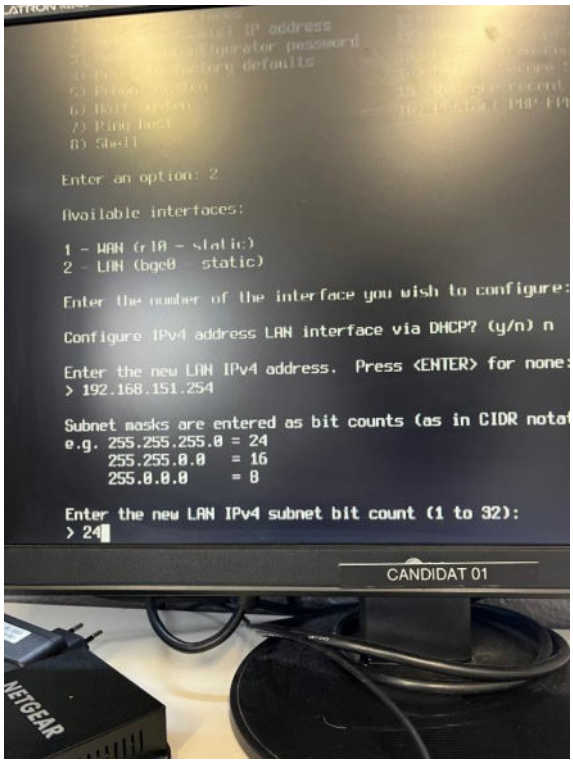
Ne pas configurer notre IP d'interface en DHCP (elle sera en IP statique)



Entrer l’adresse IP (qui servira de passerelle également pour notre réseau wifi)

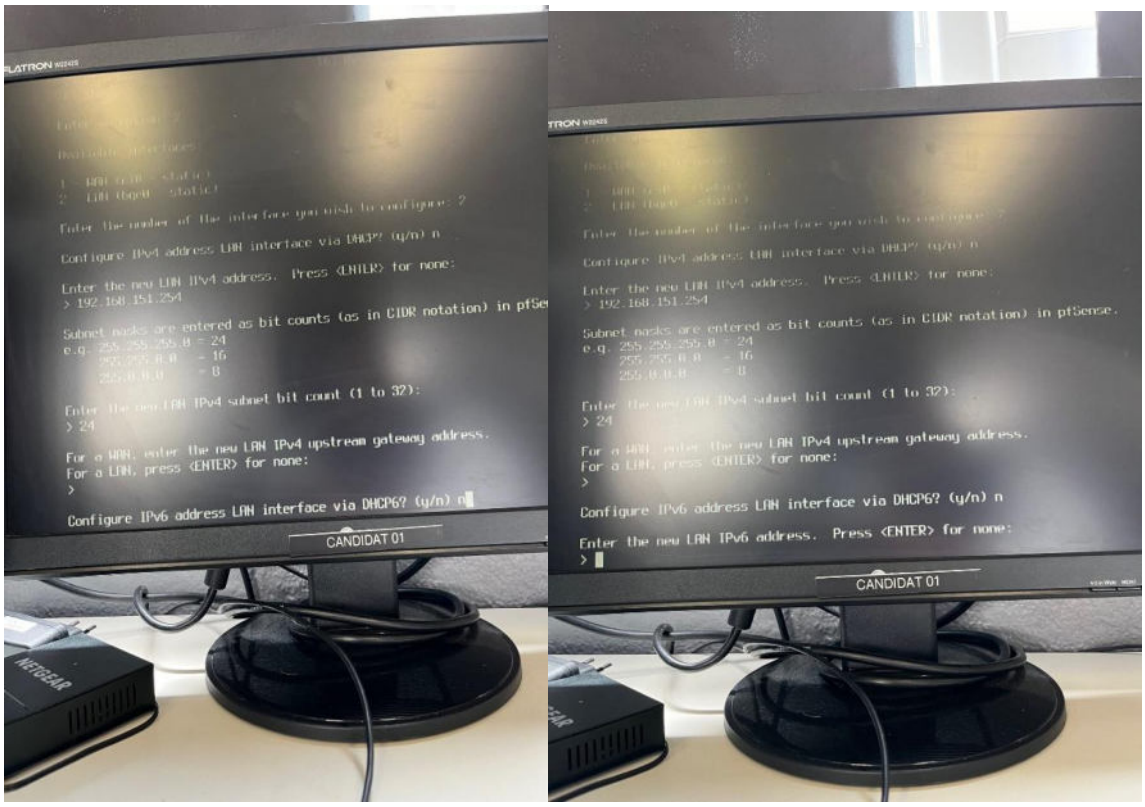


Entrer son masque

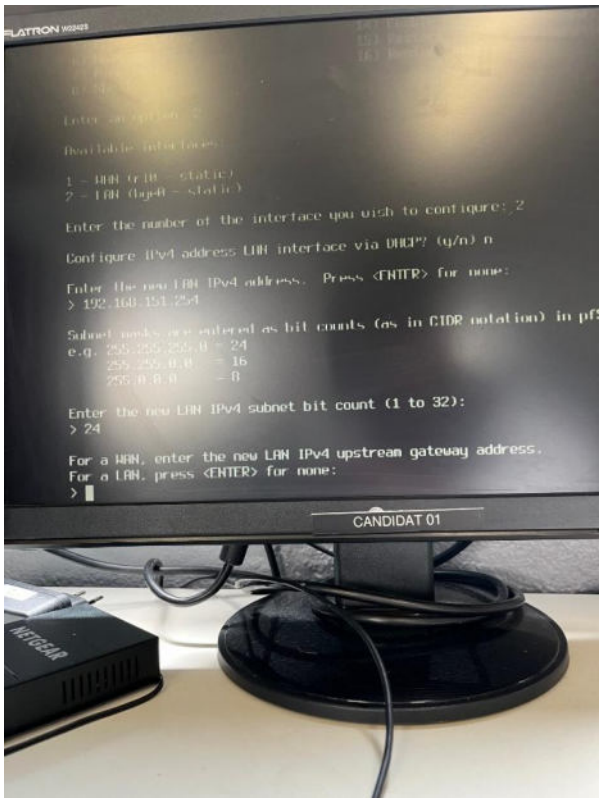


Indiquer la passerelle (nous n'en indiquerons pas étant donné que la passerelle est l'ip de notre interface bge0), appuyer sur entrée

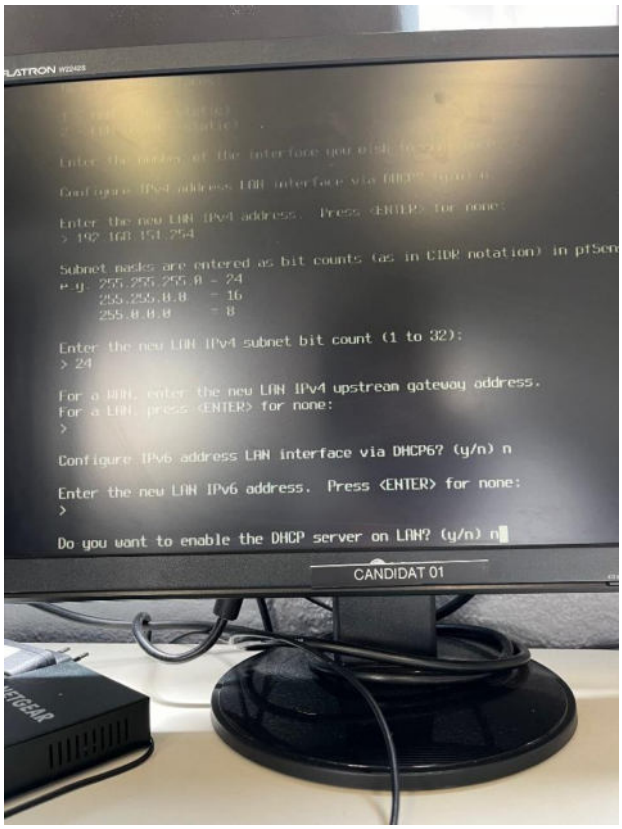
Nous ne configurerons pas d'IPV6 via DHCPV6 ni d'IPV6 en statique, nous appuyerons sur entrée



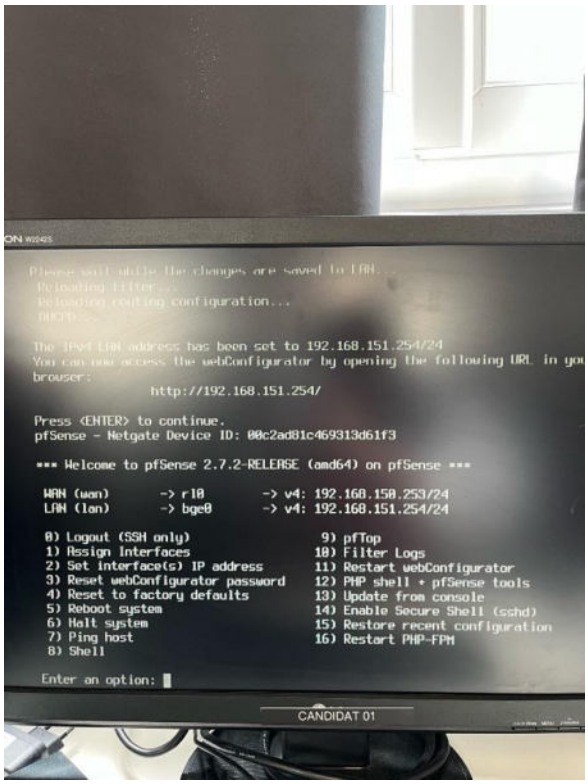
Nous ne configurerons pas de passerelle puisque nous sommes sur notre interface LAN



Désactiver le dhcp



Notre interface bge0 est alors configurée.



Etape 5 : configurer la route

Il va nous falloir deux routes :

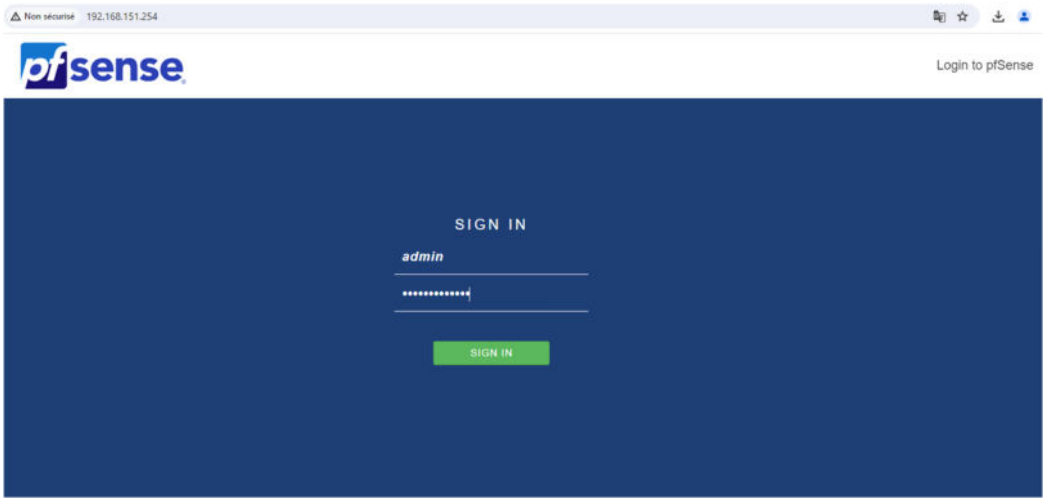
Une du Proxy vers le switch (indiquer la route vers 172.16.150.254 afin qu'il puisse joindre le switch qui lui-même joindra le réseau de sortie)

Une du switch vers le proxy (indiquer la route vers 172.16.150.253 qui permettra de joindre le réseau 151)

Une de notre box internet vers le réseau wifi 151 (de 172.18.0.1 vers le réseau 172.16.0.0)

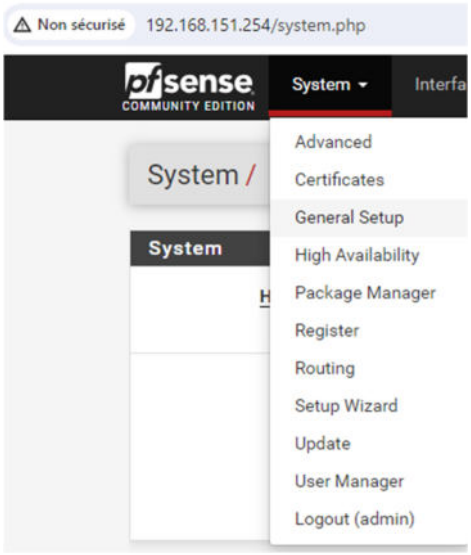
Pour configurer la première route, nous allons nous connecter à l'interface web de pfsense via l'ip de notre interface lan (bge0) qui est 172.16.150.254

Se connecter



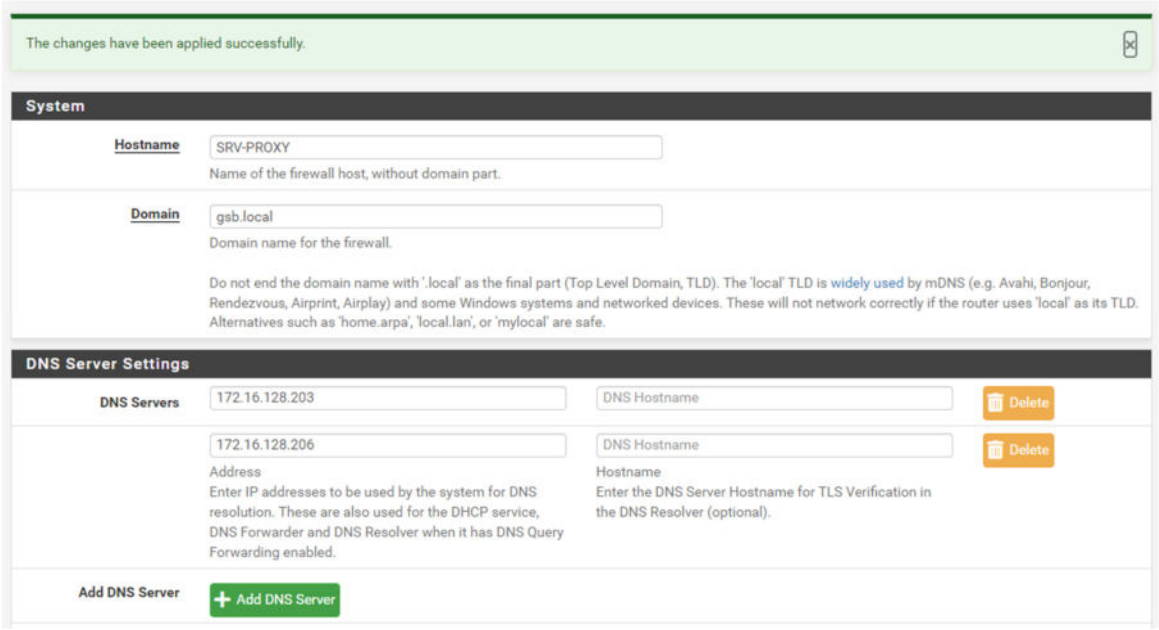
Nous en profiterons pour renommer le nom de notre machine en y incluant notre nom de domaine

Se rendre dans system puis general setup

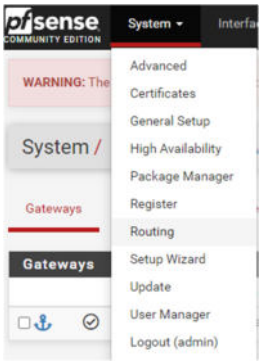


Puis nous attribuerons un nouveau nom à notre machine

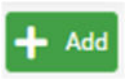
Nous en profiterons pour la joindre à notre domaine gsb.local (ainsi que l'ip des deux active directory)



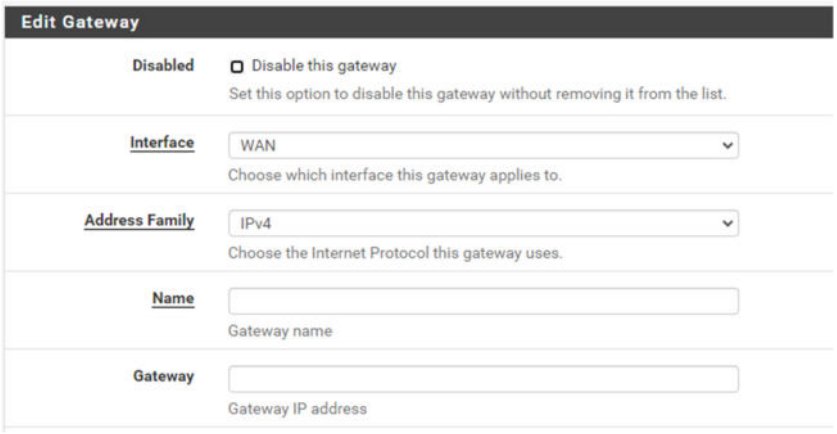
Se rendre dans system puis routing



Nous allons d’abord ajouter la passerelle, cliquer sur add

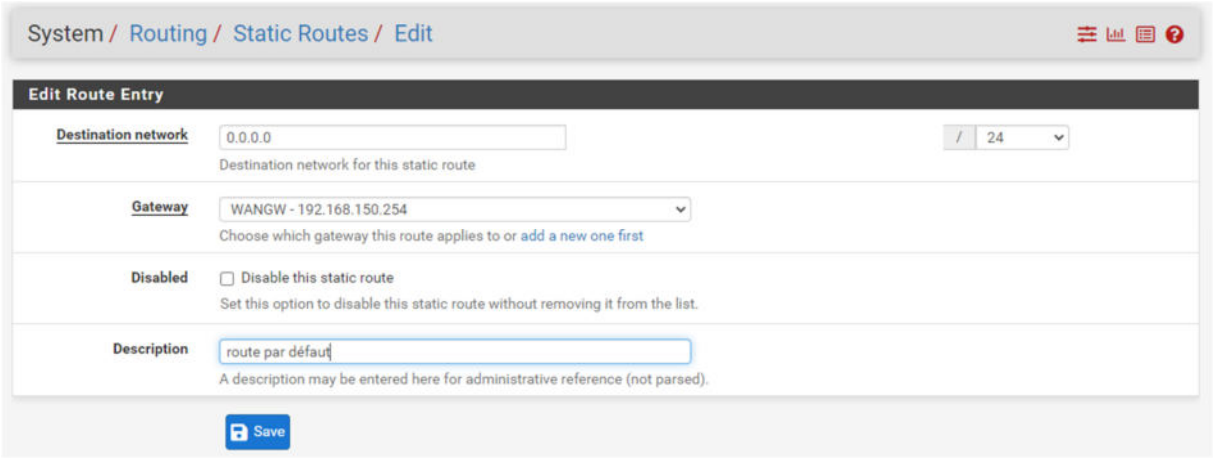


Indiquer un nom ainsi que l’IP de la passerelle puis cliquer sur save



Se rendre ensuite dans static route, cliquer sur add

Puis indiquer la route (0.0.0.0 étant la route par défaut qui permet de joindre tous les autres réseaux hormis les réseaux adjacents du proxy), avec la passerelle cisco du réseau (172.16.150.254)



Etape 6 : configurer la route sur le switch

Rentrer la commande « en » pour enable puis « conf t » pour le mode configuration

Ensuite indiquer la route vers notre réseau wifi avec la commande « ip routing 192.168.151.0 255.255.255.0 192.168.150.253» puis effectuer la commande « end » (modifier la route)

```
Switch(config)#ip route 192.168.150.0 255.255.255.0 192.168.150.253
Switch(config)#
```

Puis enregistrer la configuration avec la commande copy running-config startup-config

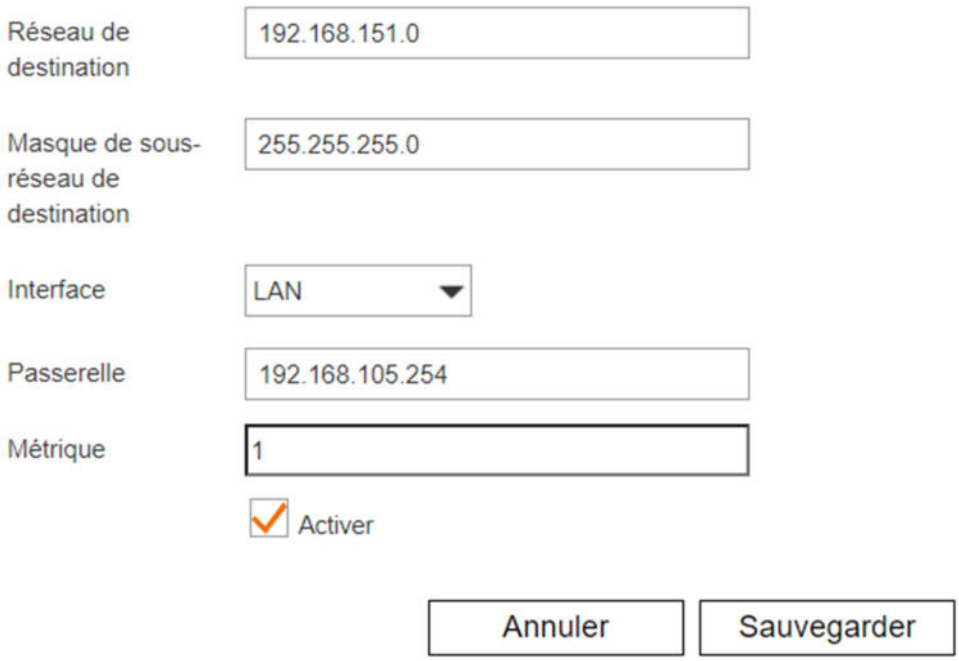
Etape 7 : configuration de la dernière route sur notre box internet

Se connecter en admin sur la box

Se rentre dans network puis routage

Créer une nouvelle route avec l'ip du réseau de destination du wifi avec la passerelle 192.168.105.254 (passerelle cisco afin que lui-même puisse joindre le réseau suivant)

Nous lui mettrons la métrique 1 (il s'agit de l'importance de la règle) puis activer notre règle et sauvegarder

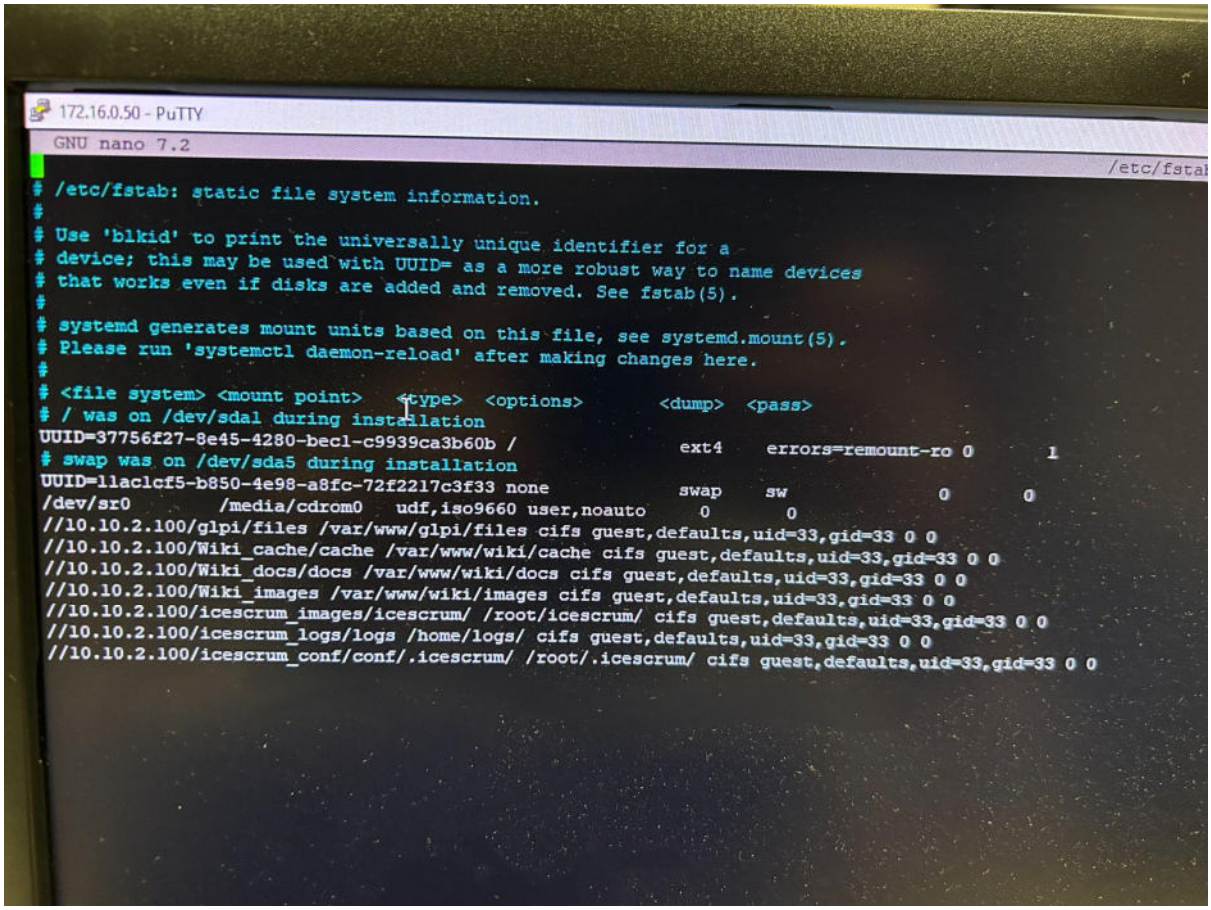


Avant de démarrer installer rsync : apt install rsync
Ensuite rendez à l'endroit du dossier ou fichier que vous voulez envoyer
Puis taper la commande :
rsync -rav /Chemin/Du/DossierSource Utilisateur@ServeurCible:/Chemin/De/Destination
Il vous demandera de taper le mot de passe de l'utilisateur, renseigner le.
Enfin, aller sur la procédure pour faire des points de montage.

1. Modifier /etc/fstab (Point de montage lancer au démarrage)
2. Ajouter :

//IP du Samba/Nom du partage/Chemin (si il y en a besoin) /CheminDu/DosierDe/Montage Format (CIFS pour Samba) guest,defaults,uid=33,gid=33 0 0 (pour pas s'embêter avec les utilisateurs)

Exemple venant du contexte :



3. Redémarrer le serveur pour actualiser les points de montages
4. Après le redémarrage taper : mount -a -v pour verifier si cela a fonctionner
5. Si l’erreur est que le format CIFS n’est pas pris en charge, installer cifs-utils en tapant apt install cifs-utils
6. Sinon l’erreur vient du chemin de partage ou du point de montage

Configuration borne WiFi :

Etape 1 :

Notre réseau WiFi sera le 172.16.150.0/24

Il faudra mettre son poste sur le même réseau que la borne WiFi (sans passerelle) et bien brancher la borne sur un port du switch non tagué relié au port lan

Se connecter via l'interface web de la borne WiFi (son ip par défaut étant 172.16.)

(Nouvelle IP 172.16.150.250/24 et masque 255.255.255.0)

La borne aura également le rôle DHCP

Etape 2 :

Modifier les accès à la borne (identifiant et mot de passe)

Nouvel identifiant : admin

Nouveau MDP : Azerty$123456

Etape 3 :

Arrivée sur l'interface de la borne

Entrer dans le menu setup et démarrer avec le setup assistant

Pour la connexion vers le WAN, elle sera en « disable »

Etape 4 :

Modifier l'adresse IP de notre routeur/borne wifi par la 172.16.150.253

Masque 255.255.255.0

Local dns 172.16.100.1

Activer le DHCP server et indiquer une étendue DHCP sur notre borne (de 50 à 150)

Etape 5 :

Changement du SSID (le premier GSB GOOGLE, le second GSB PLACE) en WPA2

MDP : Azerty$123456

Changer le nom du routeur (ROUTER-GSB), nous restons en WPA/AES

Hostname : WIFI-GOOGLE (va nous servir pour la résolution dns, puis nous rentrerons par la suite une entrée dns dans l'ad)

Nom de domaine : gsb.local

Etape 6 :

Vérifier notre configuration, ajouter les deux serveurs dns 172.16.128.203 et 206

Puis sauvegarder et appliquer les configurations

Pour avoir accès à nouveau à la borne wifi, il faudra se mettre en ip fixe sur le réseau 192.168.151.0 et rentrer l'ip de la borne 192.168.151.253 dans la barre de recherche afin d'avoir accès à son interface

Maintenant, nous allons effectuer les tests réseaux.

Nous pinguons bien nos différentes passerelles jusqu'à la sortie WAN et la résolution dns fonctionne également.

Pour finir, nous allons effectuer une règle sur le firewall dans l'onglet LAN interdisant le protocole ICMP (ping) depuis celui-ci

Pour cela, nous devrons nous rendre sur l'interface web pfsense avec l'ip lan 192.168.151.254

Se connecter avec les logs admin et pfsense

Se rendre dans firewall puis rules puis LAN

Ajouter une règle en cliquant sur add to the top list (très important de placer cette règle en haut des autres afin que le protocole ICMP soit bloqué)

En action, nous allons bloquer depuis l'interface lan le protocole ICMP depuis tous les réseaux sources vers tous les réseaux de destination (nous pouvons renseigner une description à notre règle)

Cliquer sur save puis bien penser à appliquer les changements.

Tester à nouveau le ping, celui-ci est bien bloqué.

COMMANDES SQL

Afficher les Utilisateurs :

```
SELECT User,Host FROM mysql.user;
```

Afficher qui possède les droits sur une BDD :

```
SELECT * FROM mysql.db WHERE Db = ‘my_bdd’;
```

* = Tous les users
‘my_bdd’ = Nom de la base de données

Changer de mot de passe pour un utilisateur:

```
ALTER USER toto@host IDENTIFIED BY ‘MonMagnifiqueMotDePasseTrèsSecur’;
```

Installer mariadb client et server sur les différents noeuds.

mysql_secure_installation pour configurer la sécurité des serveurs SQL

Attention : mot de passe identiques pour root

SUR LE NOEUD MASTER :

root@www:~# systemctl stop mariadb
root@www:~# nano /etc/mysql/mariadb.conf.d/50-server.cnf
(# line 27 : commenter
#bind-address = 127.0.0.1) pas sur

ajouter à la fin
[galera]
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so
wsrep_cluster_address="gcomm://"
binlog_format=row
default_storage_engine=InnoDB
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0
# nom du cluster
wsrep_cluster_name="MariaDB_Cluster"
# IP du serveur master
wsrep_node_address="Adresse du master"

root@www:~# galera_new_cluster
root@www:~# systemctl restart mariadb

SUR TOUS LES AUTRES NOEUDS

root@node01:~# nano /etc/mysql/mariadb.conf.d/50-server.cnf
(# line 27 : commenter
#bind-address = 127.0.0.1) pas sur

ajouter à la fin
[galera]
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so
# Donner toutes les IP du cluster

wsrep_cluster_address="gcomm://adresse du master,adresse du slave"
binlog_format=row
default_storage_engine=InnoDB
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0
# Même nom de cluster
wsrep_cluster_name="MariaDB_Cluster"
# IP du noeud en cours de configuration
wsrep_node_address="adresse du slave"

root@node01:~# systemctl restart mariadb

RETOUR SUR LE MASTER

root@www:~# nano /etc/mysql/mariadb.conf.d/50-server.cnf
# ajouter toutes les IP des noeuds du cluster
wsrep_cluster_address="gcomm://adresse du master,adresse du slave"

root@www:~# systemctl restart mariadb
POUR TESTER :

sur n'importe quel noeud, on entre dans la commande MySQL avec la commande "mysql"
Puis :
show status like 'wsrep_%';

On regardera la ligne "wsrep_local_state_comment"

Si elle indique "Synced" les noeuds sont synchronisés