Documentation

OPNSense

BTS SIO SISR | IIA Laval

Eythan Roncier-Lemée
04/04/2025

Table des matières

1. OPENNEBULA 2

1.1. Prérequis 2

1.2. Environnement Réseau 3

1.3. Création d'une machine OPNsense 4

1.4. Création d'une machine Windows 10 6

2. WINDOWS 10 8

2.1. Changement du nom d'hôte 8

2.2. Réglage de l'adresse IP 10

2.3. Vérification de la connectivité 12

3. OPNSENSE 13

3.1. Installation 13

3.2. Configuration des interfaces 17

3.3. Configuration des IP 18

3.4. Configuration par navigateur 19

3.5. Définition des interfaces 22

3.6. Mise à jour 23

3.7. Gestion utilisateur 26

3.8. Configuration du pare-feu 28

3.8.1. Ajout d'une passerelle 28

3.8.2. Ajout d'une route 29

3.8.3. Ajout d'un alias 30

3.8.3.1. Alias pour le serveur GLPI 30

3.8.3.2. Ajout d'un alias pour le réseau Wi-Fi de l'école 31

3.8.3.3. Ajout d'un alias pour les routeurs 32

3.8.4. Gestion des règles du pare-feu 33

3.8.4.1. Contexte 1 34

3.8.4.2. Contexte 2 35

3.8.5. Test de la règle du contexte 1 36

3.9. Commandes Supplémentaires 38

1. OPENNEBULA

1.1. Prérequis

OPNsense :

Ce logiciel est défini comme un pare feu c'est lui qui va vérifier si une connexion sortante ou entrante est légitime ou non et la bloquer ou non selon les paramètres définis par l'utilisateur. Pour fonctionner il a besoin au minimum de :

Processeur	1Ghz, 2 cœurs
RAM	2 GB
Stockage	30 GB recommandé

Windows 10 (console) :

Windows 10 est un système d'exploitation sortie en 2017 par Microsoft il tombera obsolète en octobre 2025 au vu de sa vétusté et de l'envie de Microsoft d'arrêter de le maintenir à jour. Pour fonctionner il a besoin au minimum de :

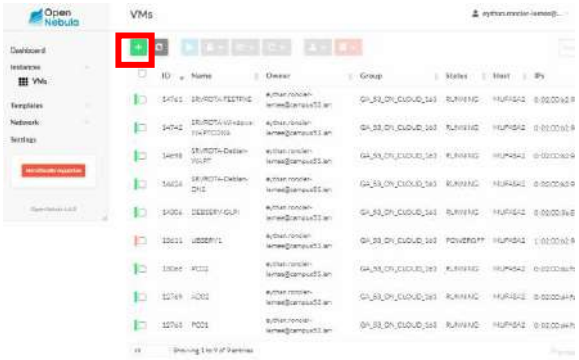
Processeur	1Ghz, 2 cœurs
RAM	2 GB
Stockage	30 GB recommandé
Carte Graphique	Carte supportant DirectX 9 ou ultérieur
Affichage	Résolution d'affichage de 800 x 600

1.2. Environnement Réseau

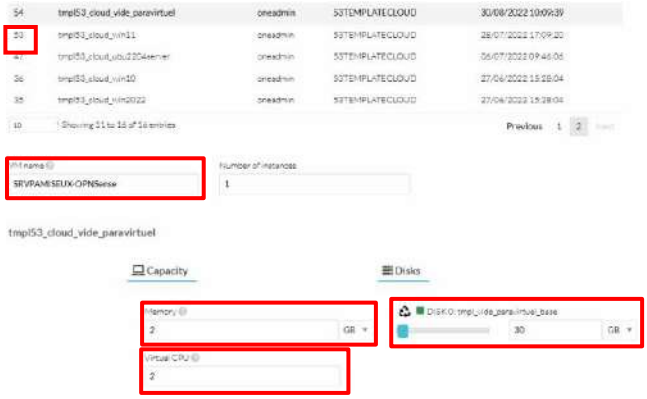
ID	Nom VLAN	MAC	Type	Type Adressage	IP
0	Vlan-WAN-CCI53	02:00:ba:3b:b6:ce	WAN	DYNAMIQUE DHCP	10.192.0.0
1	Vlan-virtlab-0690	02:00:3b:87:1d:9d	LAN	Statique	10.192.190.70
2	Vlan-virtlab-0691	02:00:b2:98:58:e2	DMZ	Statique	10.192.191.70
3	Vlan-virtlab-0692	02:00:d4:fd:a3:0c	SRV	Statique	10.192.192.70

ID	Nom VLAN	Réseau	Passerelle	DNS	Type adressage
2910	Vlan-virtlab-0690	10.192.190.0	10.192.190.254	10.223.255.2	Statique
2909	Vlan-virtlab-0691	10.192.191.0	10.192.191.254	10.223.255.2	Statique
2908	Vlan-virtlab-0692	10.192.192.0	10.192.192.254	10.223.255.2	Statique
501	Vlan-WAN-CCI53	10.192.0.0	Dynamique	Dynamique	DHCP

1.3. Création d'une machine OPNsense

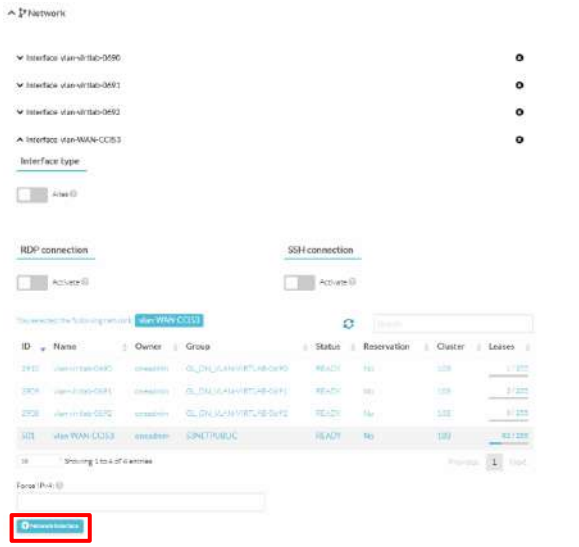


- Cliquez sur le « + » celui-ci va permettre la création d'une nouvelle machine.



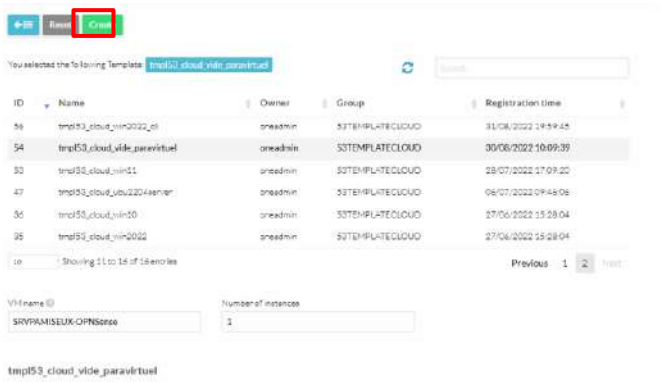
- Sélectionnez le modèle qui porte l'ID 54 ou le nom « tmpl53_cloud_vide_paravirtuel ».

- Choisir le nom de la machine et faire correspondre les caractéristiques minimums requis par OPNsense (2gb RAM, 30gb de stockage, 2 cœurs).

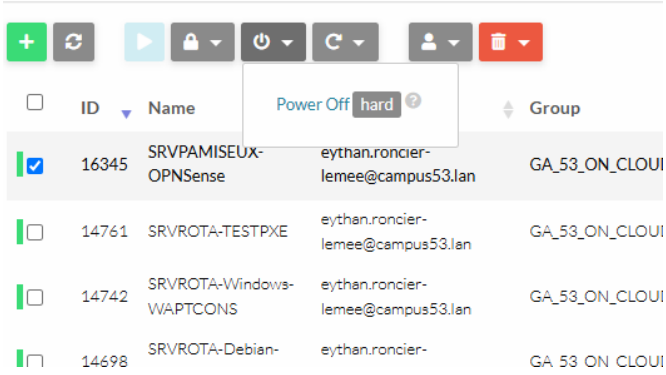


- En défilant la page vous vous retrouverez à la configuration des interfaces. Il faudra bien veiller à tous les sélectionner.

- Pour ce faire il suffit de sélectionner une interface dans le tableau puis de cliquer sur le bouton entouré en rouge.



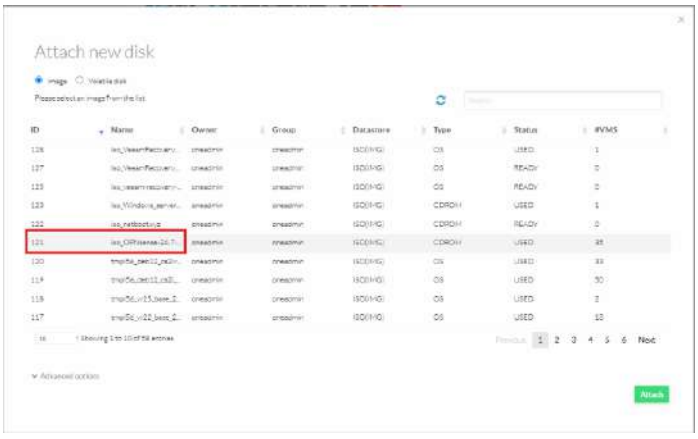
- Lorsque vous aurez sélectionné la dernière interface il suffira de cliquer sur le bouton « Create » ou créer, afin de lancer la procédure de création de la machine.



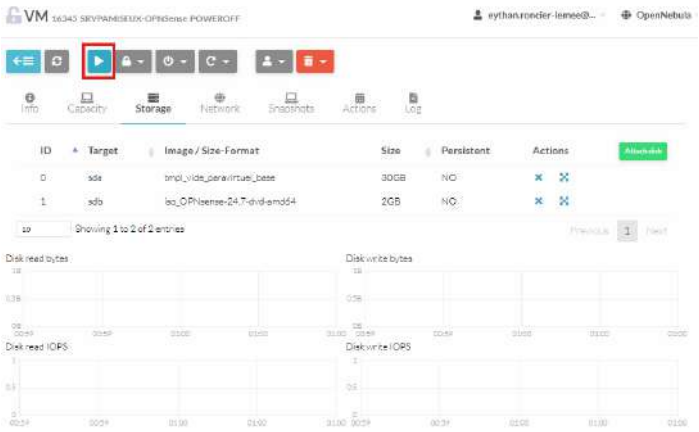
- Une fois que la machine est en état « RUNNING » Il faudra l'éteindre en la sélectionnant puis appuyez sur le bouton d'arrêt présent sur l'accueil d'OpenNebula et enfin de cliquer sur « Power Off hard ».



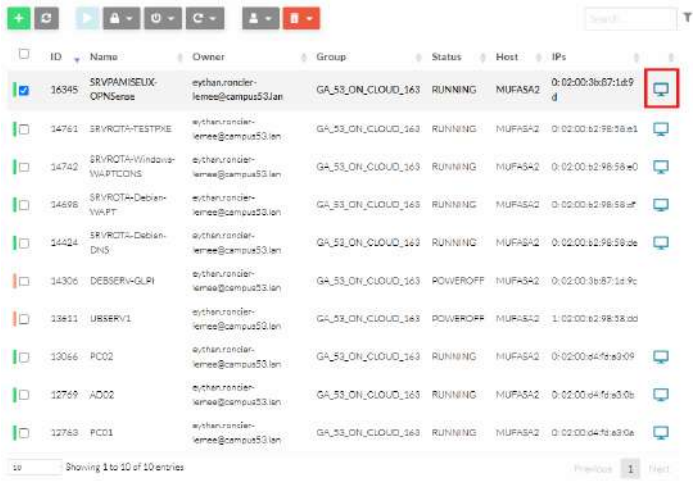
- Double-cliquez sur la machine afin de se rendre dans l'onglet « Storage » et d'enfin attacher le disque qui servira pour le démarrage de la machine car pour l'instant c'est une coquille vide.



- Le disque 121 possède donc l'installation du système permettant de mettre en place le pare-feu. Nous allons donc l'utiliser.

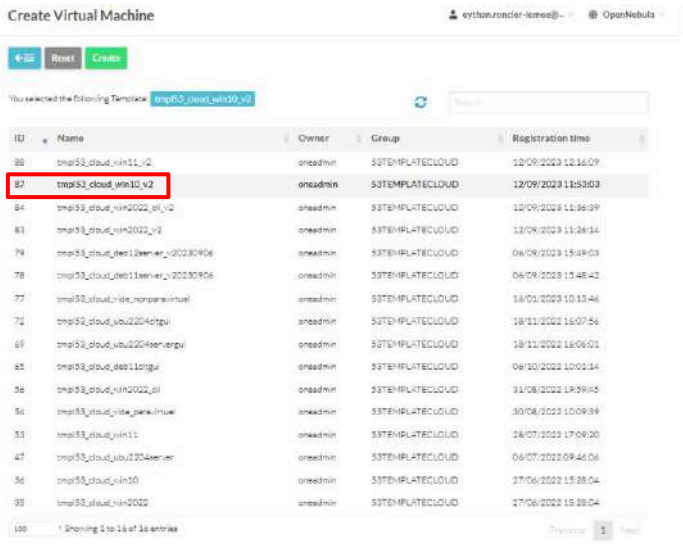


- Le disque maintenant attaché on va pouvoir donc démarrer notre machine afin de commencer l'installation.

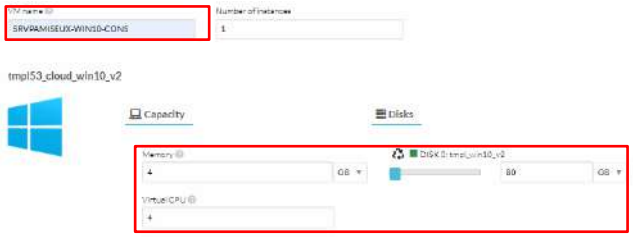


- Afin de pouvoir accéder de manière graphique à l'installation il va nous être utile d'avoir une supervision et c'est pour cela qu'il faudra cliquer sur cette icône d'écran présent sur l'accueil d'OpenNebula.

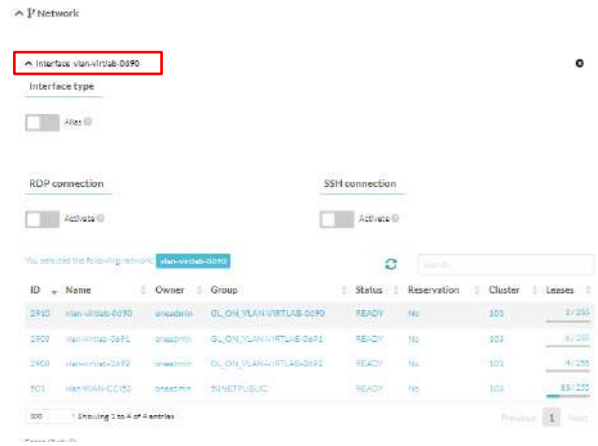
1.4. Création d'une machine Windows 10



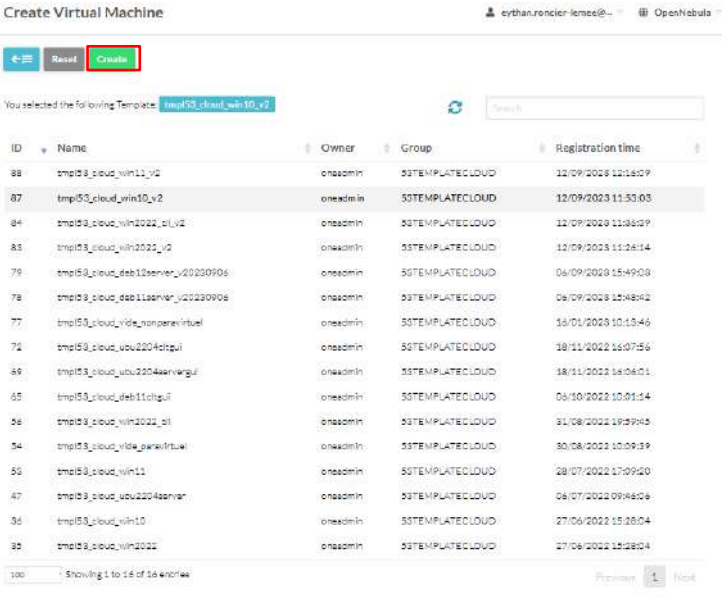
- Même chose que pour la machine OPNsense nous allons utiliser OpenNebula afin de pouvoir créer notre console qui nous servira pour la suite à la configuration de notre pare-feu.
- La première étape est la même que pour notre machine OPNsense. Cliquer sur le « + » présent sur l'accueil puis sélectionner la ligne **87** ou « **tmpl53_cloud_win10_v2** ».



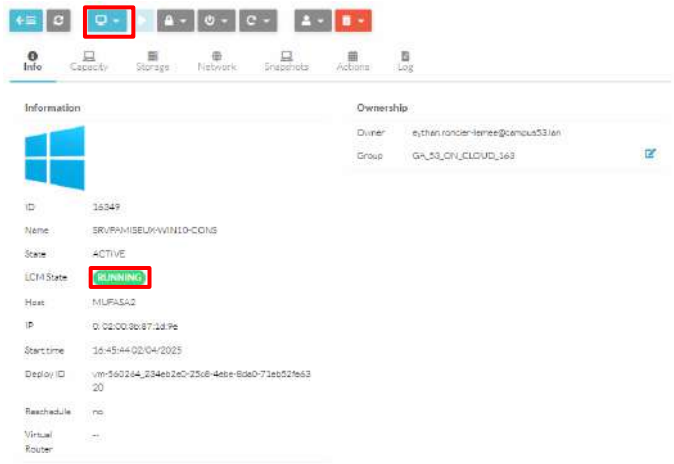
- Il faudra nommer la machine et lui définir ses caractéristiques (RAM, CPU, Stockage, Réseau).



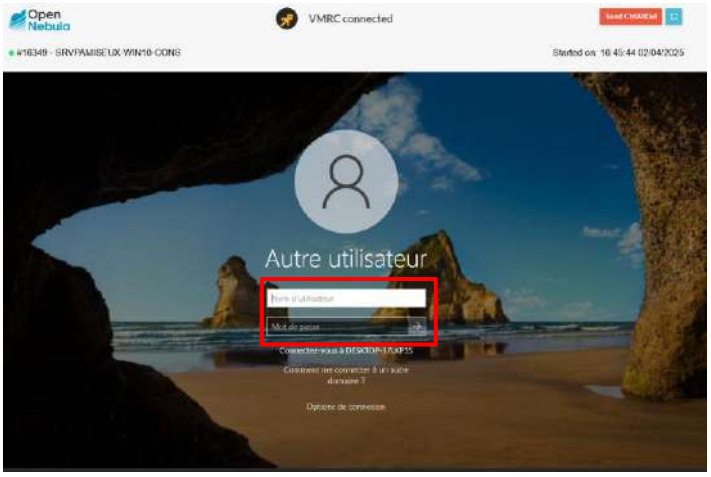
- Afin de pouvoir accéder de manière graphique à l'installation il va nous être utile d'avoir une supervision et c'est pour cela qu'il faudra cliquer sur cette icône d'écran présent sur l'accueil d'OpenNebula.



- Même chose que pour la machine OPNsense nous allons utiliser OpenNebula afin de pouvoir créer notre console qui nous servira pour la suite à la configuration de notre pare-feu.
- La première étape est la même que pour notre machine OPNsense. Cliquer sur le « + » présent sur l'accueil puis sélectionner la ligne **87** ou « **tmpl53_cloud_win10_v2** ». Pour enfin cliquer sur « **Create** ».



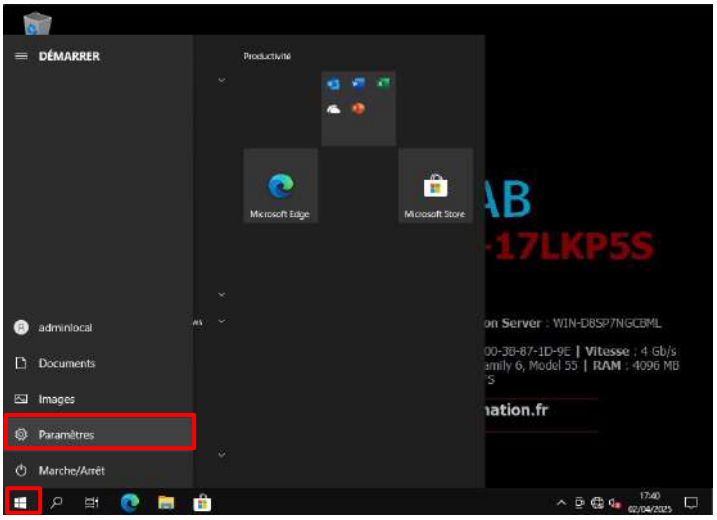
- Lorsque la machine passe en état « RUNNING » c'est qu'elle est en fonctionnement de ce fait l'écran s'affiche sur la ligne supérieur cliquer dessus fera apparaitre « **VMRC** », qui nous sera utile pour la supervision.



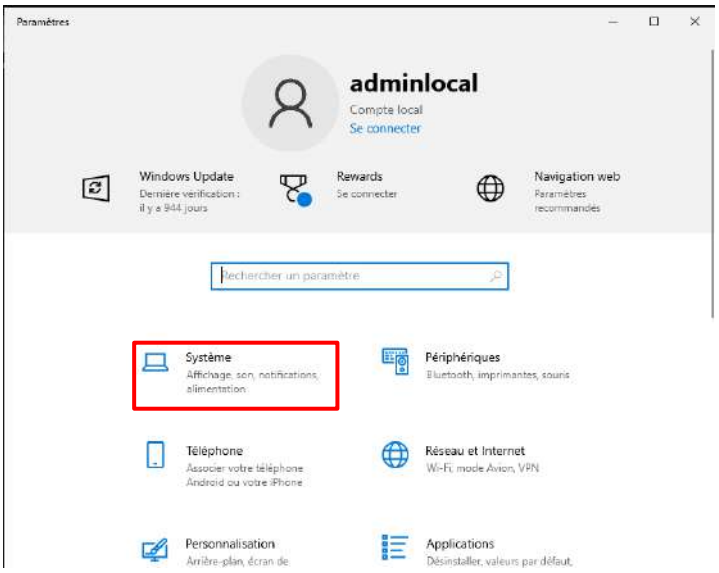
- L'avantage avec ce système c'est qu'on n'a pas besoin de le configurer ou du moins beaucoup moins qu'un système classique installé via une image.
- L'utilisateur est « adminlocal », le mot de passe est « Not24get ».

2. WINDOWS 10

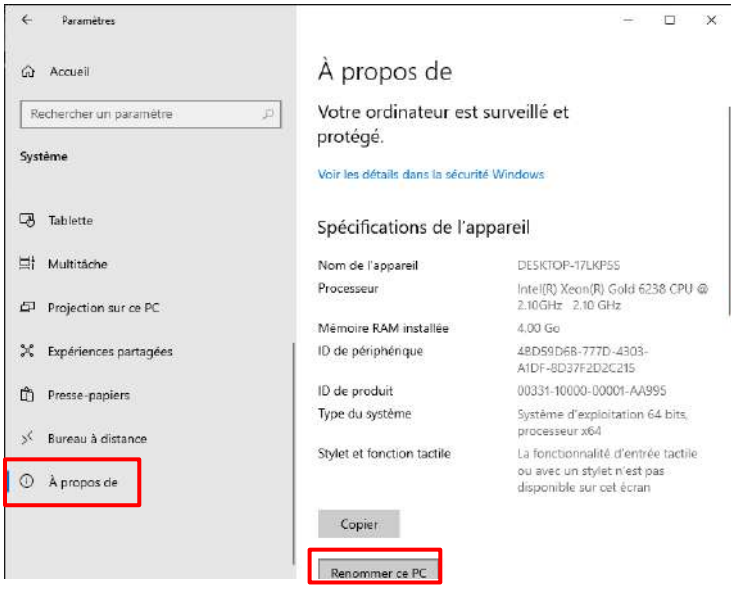
2.1. Changement du nom d'hôte



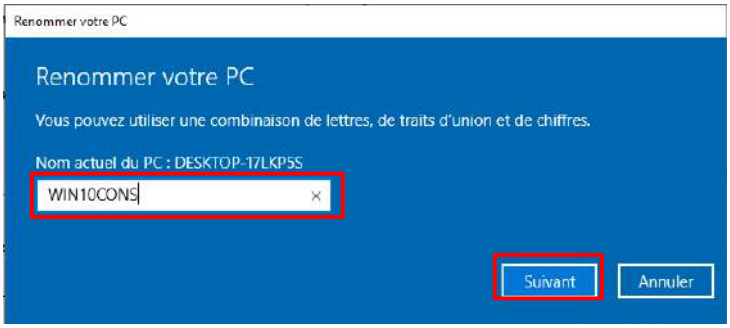
Afin de reconnaître la machine il est nécessaire de la renommer Pour ce faire il faut se rendre dans le menu Windows puis cliquer sur paramètres ou effectuer la combinaison Windows + i.



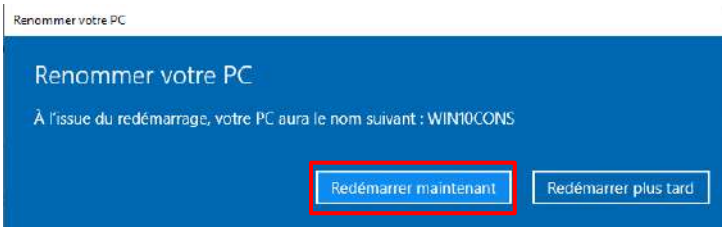
- Sélectionnez « Système ».



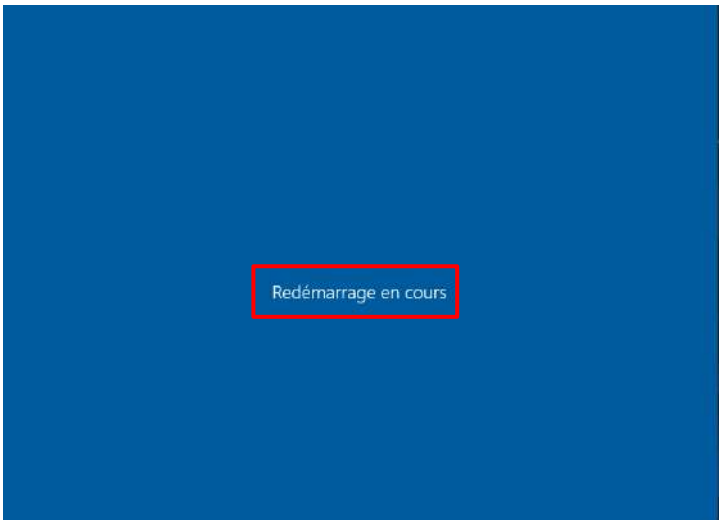
- « A propos de » puis « Renommer ce PC ».



- Le précédent nom s'affiche et dans ce champ de texte vous serez invité à entrer un nouveau nom.

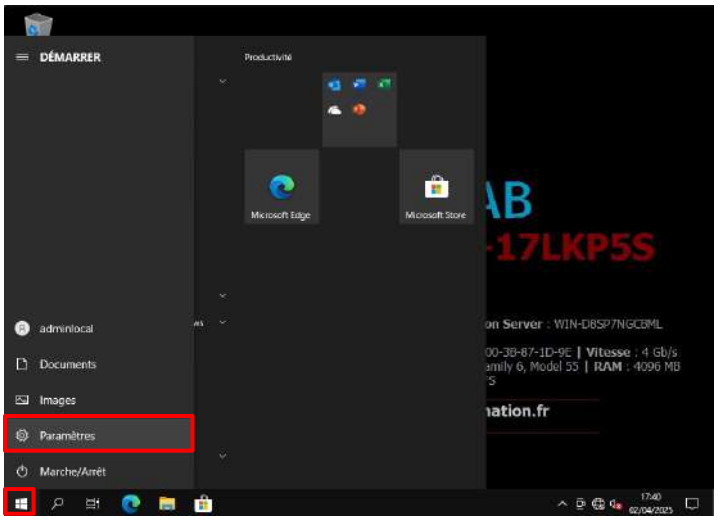


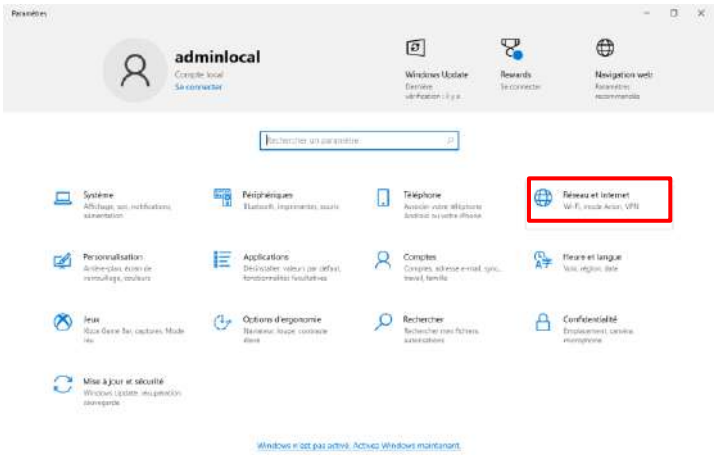
- Pour que le changement soit effectif il faudra faire « Suivant » et redémarrer le poste.



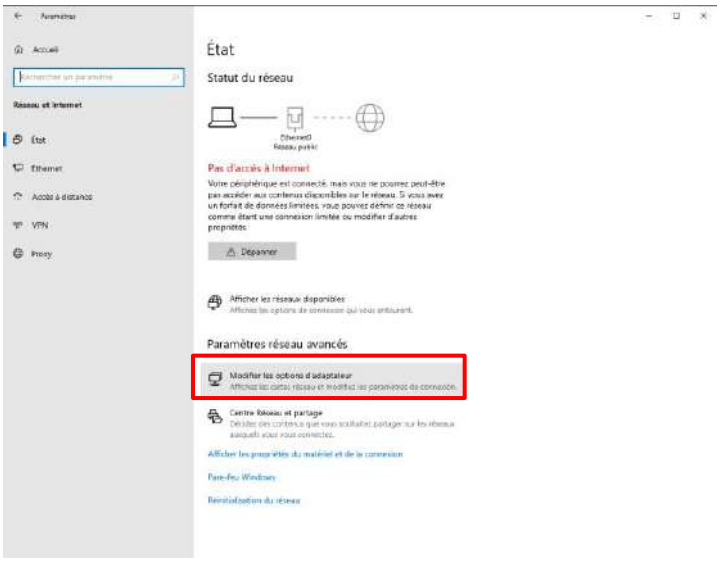
- Après le redémarrage le nouveau nom apparaitra dans les paramètres.

2.2. Réglage de l'adresse IP

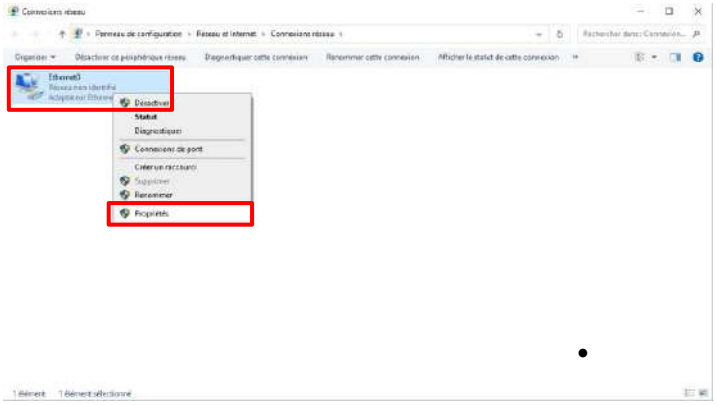




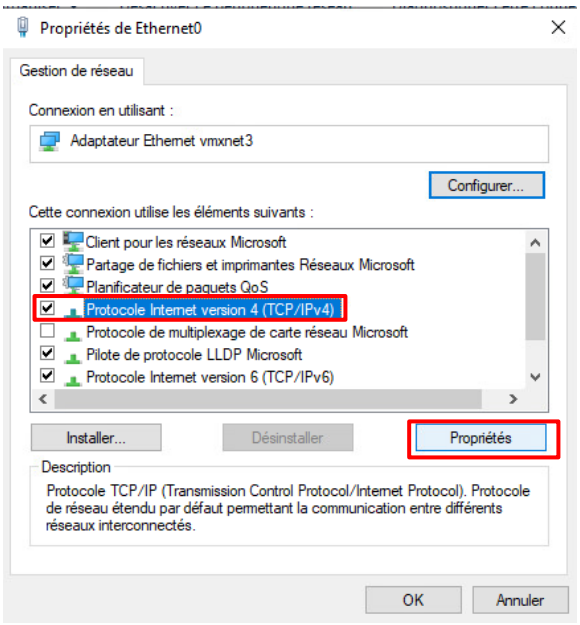
Dans ce réseau local, il sera nécessaire de régler l'adresse de votre machine. Pour ce faire, il faudra se rendre encore une fois dans le menu Windows, puis dans « Paramètres ». Afin de se rendre par la suite dans « réseaux et Internet ».

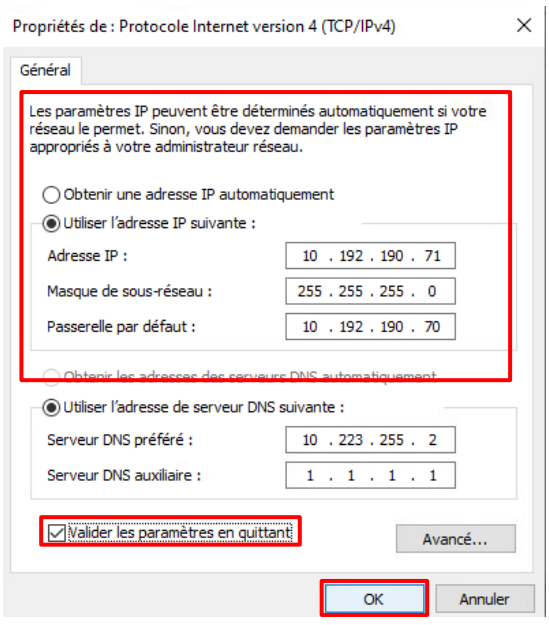


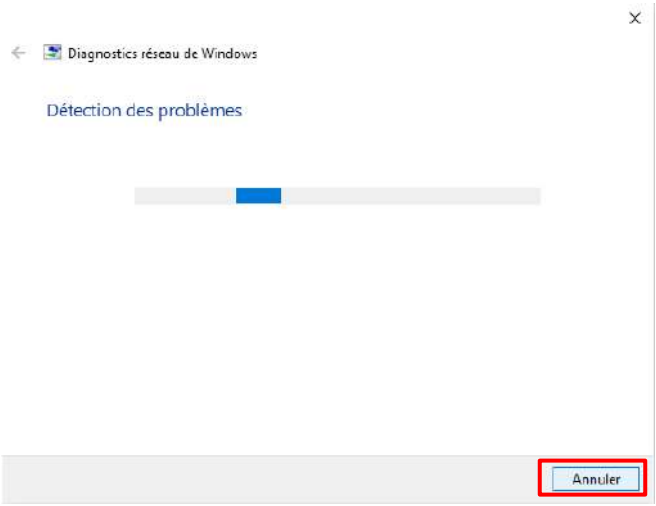
- Désormais dans l'onglet « État » présent à gauche.
- Dans le volet de droite, il y aura une option « Modifier les options d'adaptateur ».



- Faire un clic droit sur la carte réseau qui nous intéresse puis se rendre dans « Propriétés ».
- Sélectionner « protocole Internet version 4 (TCP/IPv4)
- Cliquez encore une fois sur « Propriétés ».
  Cochez « Utiliser l'adresse IP suivante » et entrez les informations de votre réseau.

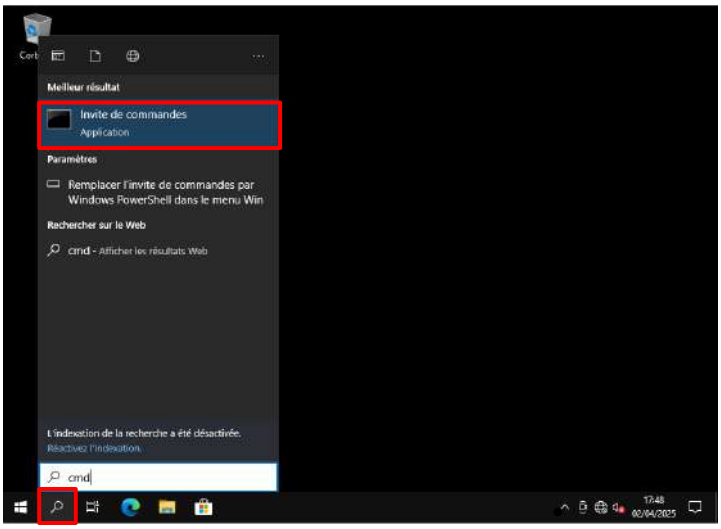




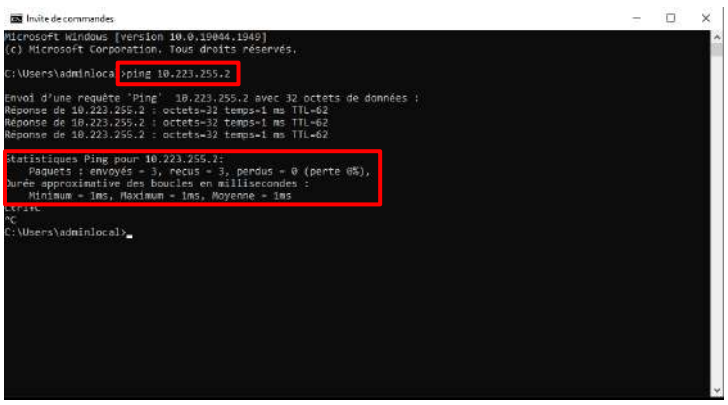


- Une fois terminé cette fenêtre de détection des problèmes s'affiche Il suffira de cliquer sur « Annuler » car en vérité aucun problème ne sera détecté.

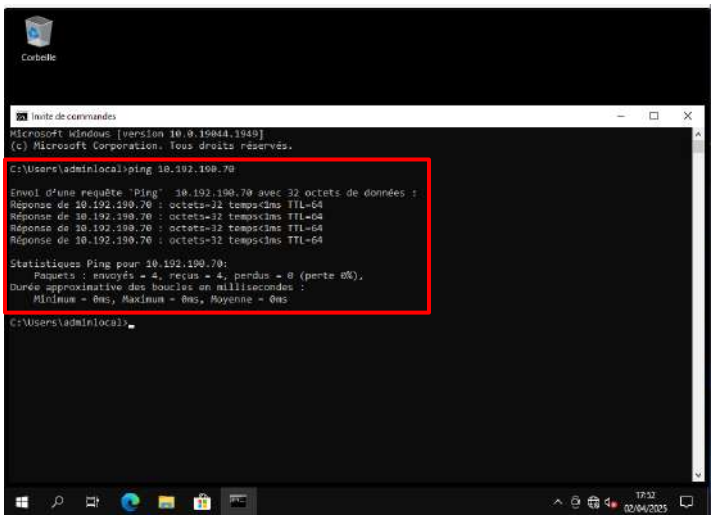
2.3. Vérification de la connectivité



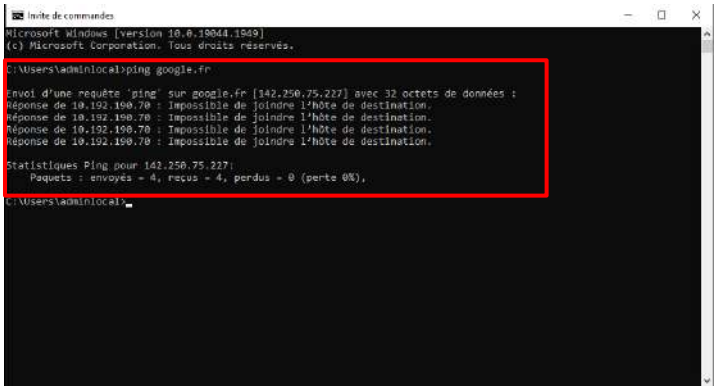
- Afin de vérifier que notre machine se connecte bien à notre passerelle ainsi qu'à notre pare feu il sera nécessaire d'effectuer un test de connectivité.
- Cliquez sur l'icône de loupe présent en bas de votre écran.
- Rechercher « CMD » et enfin double cliquer sur « invite de commandes ».



Sur cette fenêtre on va effectuer la commande « ping » qui va nous donner l'information de savoir si notre périphérique est joignable ou non via le protocole ICMP.



- Le pare-feu est joignable par la console.



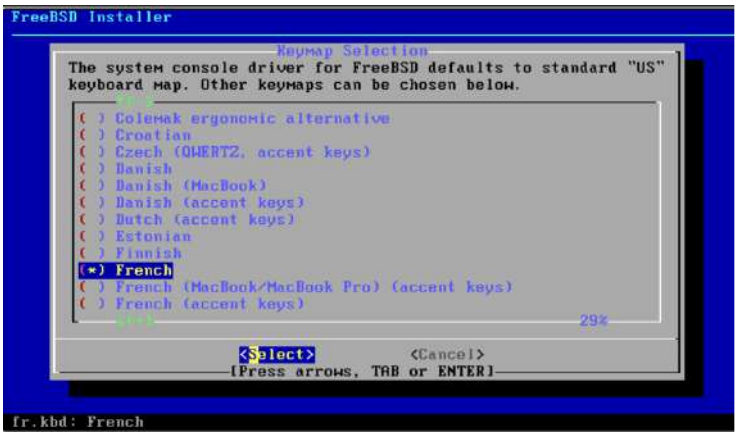
- Mais le réseau externe n'est pas joignable, toutefois ce problème sera résolu après configuration terminée du pare-feu.

3. OPNSENSE

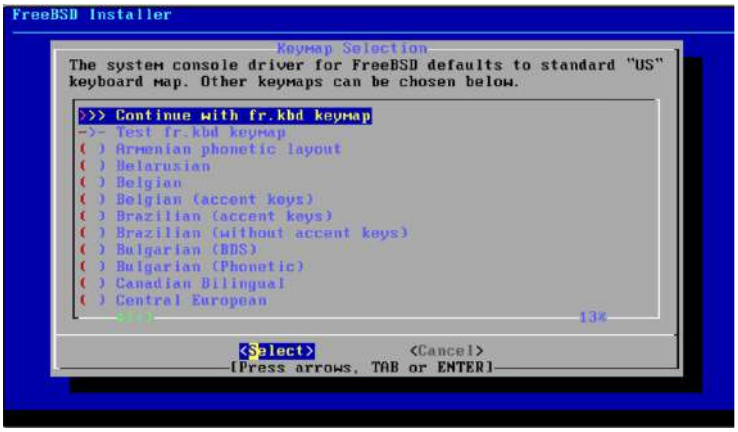
3.1. Installation



- L'installation d'OPNsense s'effectue en deux étapes la première, sur la machine, la deuxième par un navigateur web.
- A cette étape il faudra se connecter via les identifiants suivants :
  Login : installer
  MDP : opnsense
  (Attention : le clavier est en qwerty, le a et le q sont inversés).



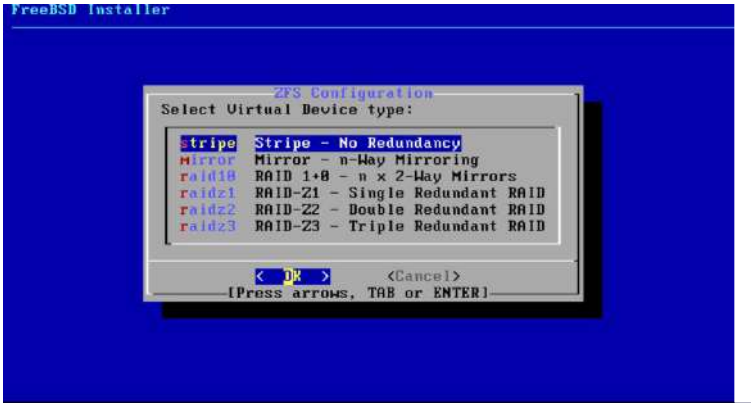
- Une fois connecté il faudra choisir la langue d'installation.
- Pour naviguer de ce menu on utilise **les flèches**. **TAB** permet de choisir « Select » ou « Cancel ». **ESPACE** permet de cocher. **ENTRER** permet de confirmer le choix.



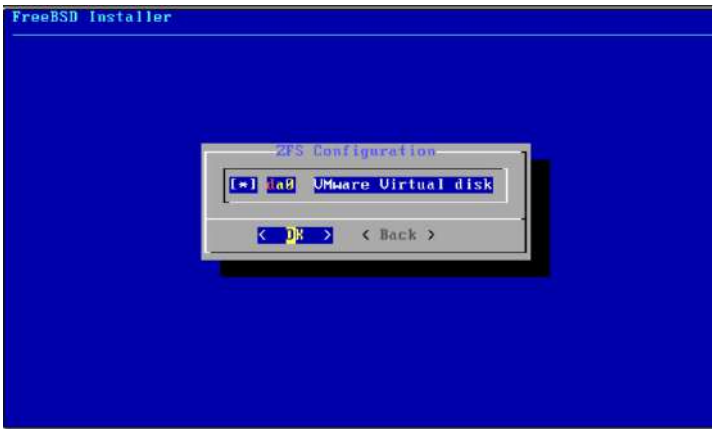
- Une fois la langue choisie il faudra remonter dans le menu afin de confirmer le choix « **Continue with fr.kbd keymap** ».



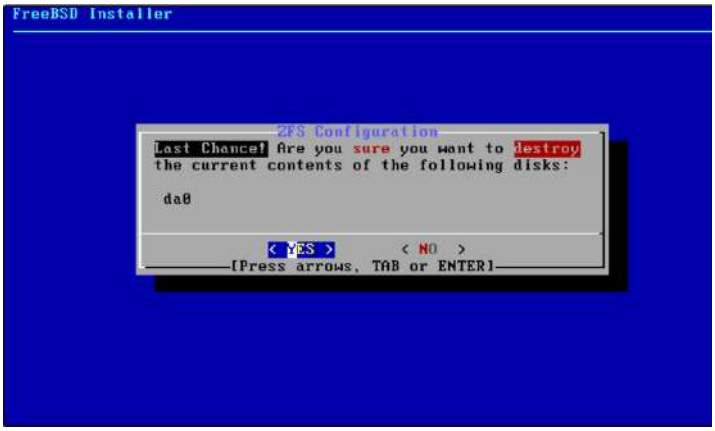
- Cette étape permet de choisir le modèle de formatage, on laisser celui de base.



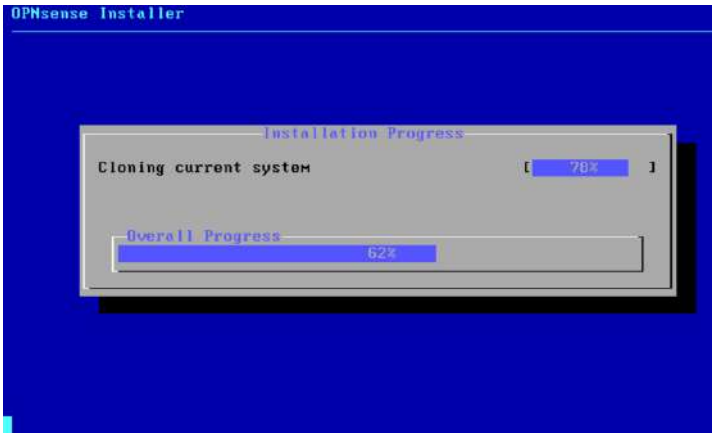
Ici, ont choisi le modèle de stockage cela permet de choisir si on souhaite de la redondance ou non dans notre cas pas besoin on laisse le choix de base.



- On coche le disque où l'on souhaite installer notre système.



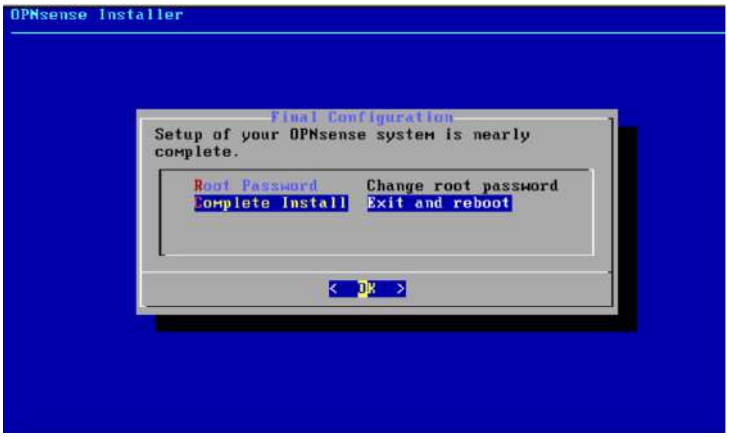
- On double vérifie si le disque choisi est bien le bon autrement on peut revenir à l'étape précédente.



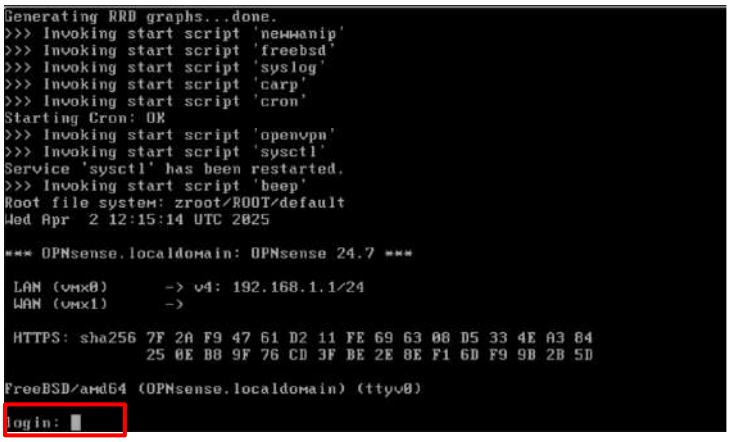
- On laisse le programme d'installation faire son job et on se fait couler un café pour la suite.



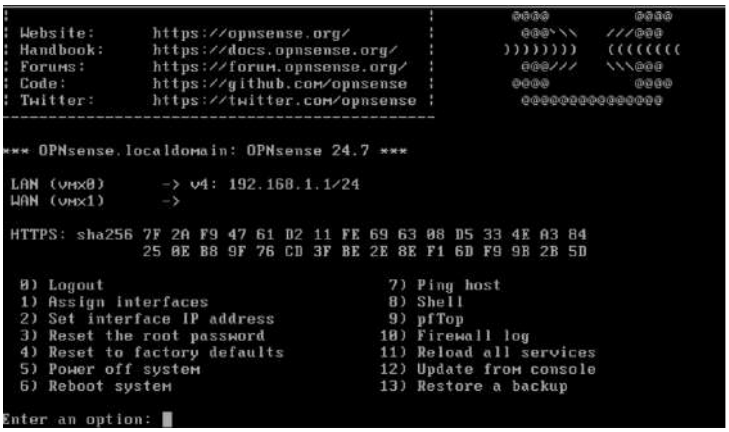
- A cette étape on va changer le mot de passe de l'utilisateur « root » on presse donc la touche ENTRER.
- On place deux fois le mot de passe dans les champs comme demandé afin de vérifier s'il y a une faute de frappe dans celui-ci.



- On peut désormais dire au programme qu'on a finis la mise en place du système.
- La machine redémarre.

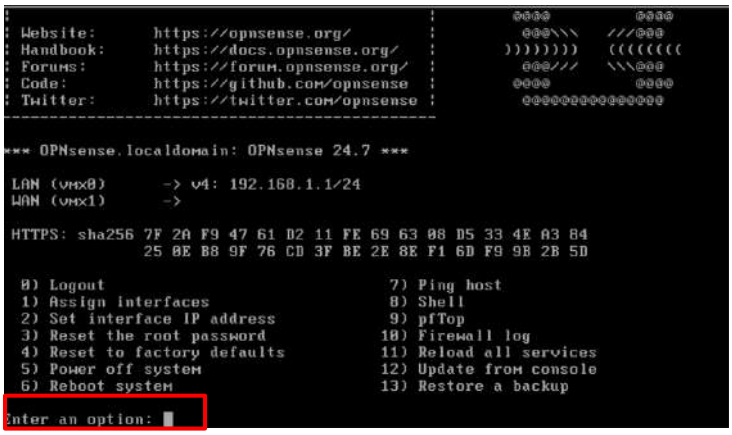


- Devant cet écran il faudra entrer les accréditations de l'utilisateur « root » afin de continuer la configuration des interfaces réseau.

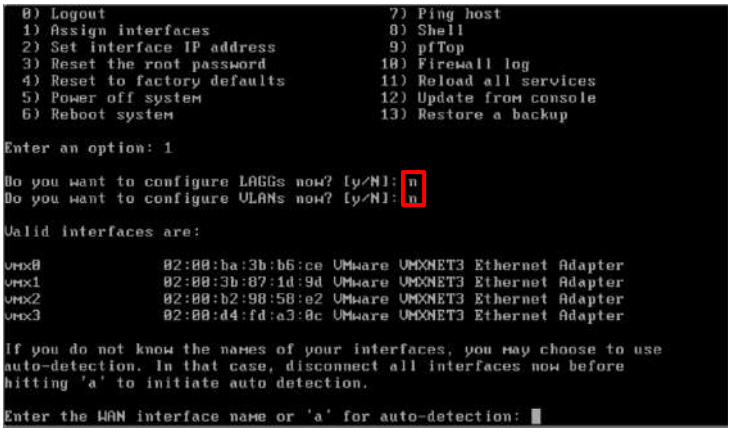


Bravo ! Le système est installé mais le plus dur arrive par la suite.

3.2. Configuration des interfaces

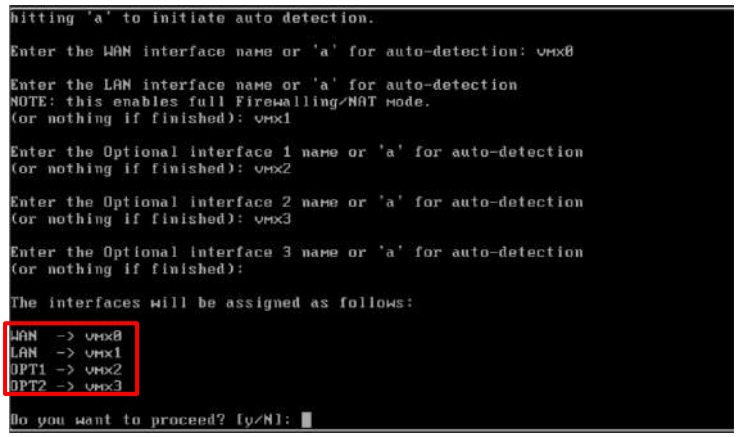


- Une liste de choix apparait on va commencer par assigner les interfaces (dire au système que tel interfaces sert à tel réseau)
- On entre donc le choix 1, le choix 0 étant destiné à se déconnecter.



- On est invité à configurer le LAGG et les VLAN pour l'instant on va dire non en entrant la lettre « n » dans les propositions.

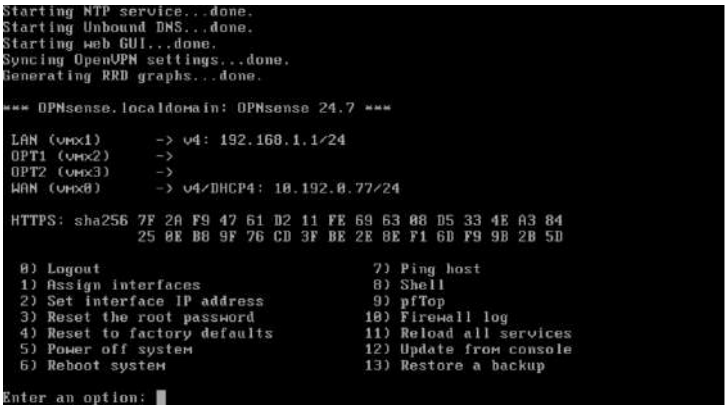
- Le système nous demande désormais de choisir l'interface considéré comme WAN autrement dit celle qui va sur internet.



- Après avoir énoncé les diverses interfaces et leurs usages au système on se retrouve avec une représentation.

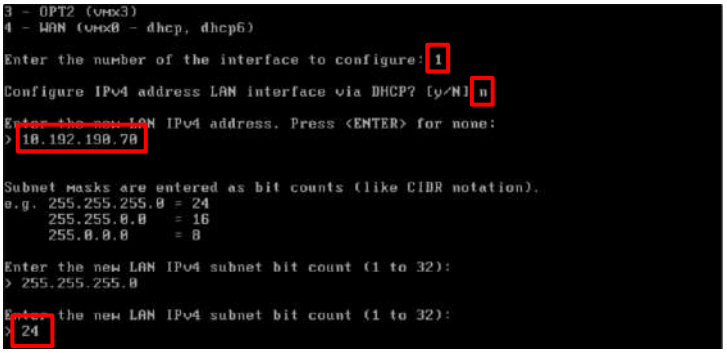
  On confirme cela par la lettre « y ».

3.3. Configuration des IP



- Les interfaces définis et leurs usages énoncés on va leurs assigner une adresse IP, passerelle, et masque de sous-réseau.

- Pour ce faire, on va choisir d'entrer le chiffre « 2 ».

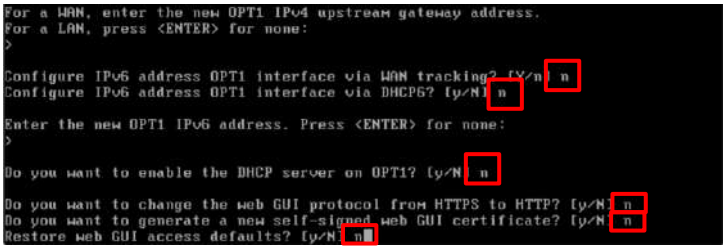


- On choisit le numéro de l'interface.

- On lui dit qu'on n'a pas de DHCP sur ce réseau.

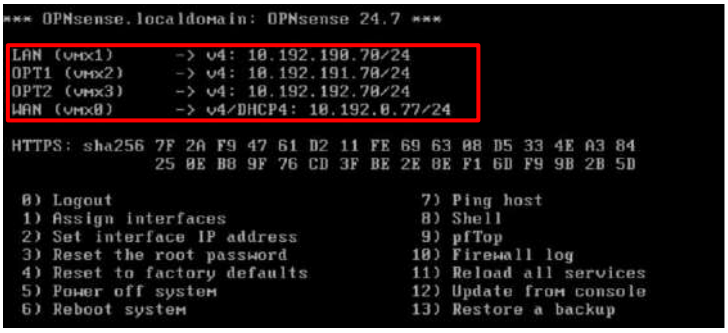
- On lui indique l'adresse IP.

- Le masque de sous-réseau.



- On ne souhaite pas configurer de DHCP en IPv6 qui est la nouvelle norme d'adresse.

- On ne souhaite pas activer de serveur DHCP.

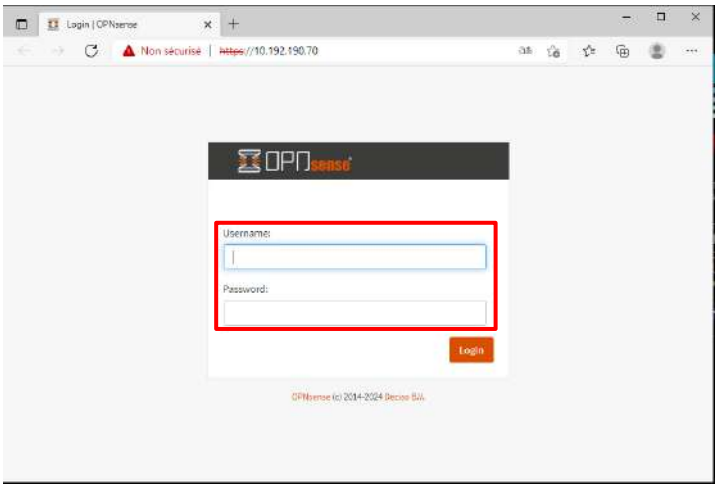


- On ne souhaite pas activer de serveur DHCP.

- On indique « n » pour ne rien configurer en supplément.

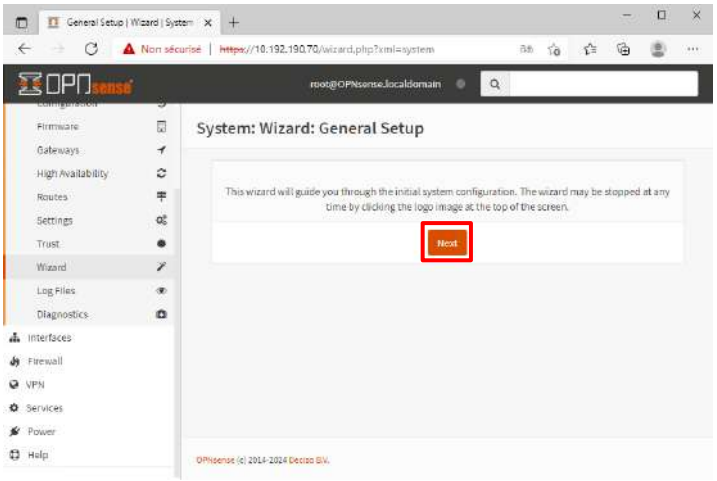
  Voilà ce que ça donne une fois configurer.

3.4. Configuration par navigateur

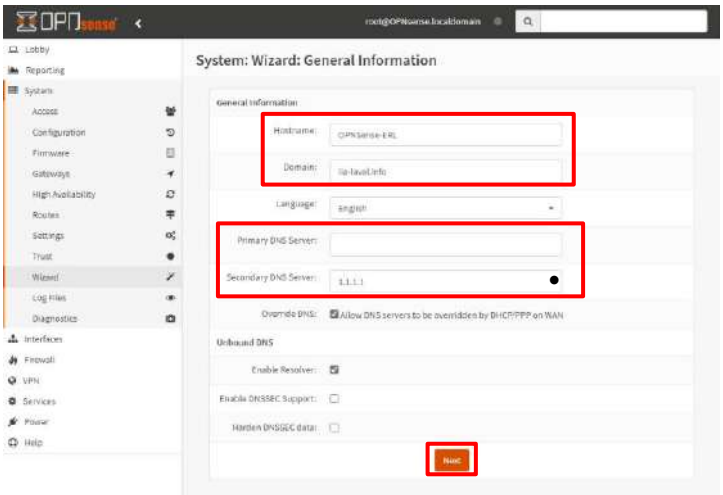


- On entre dans la phase de configuration par navigateur.

- Il faudra rentrer les identifiants de l'utilisateur « root ».



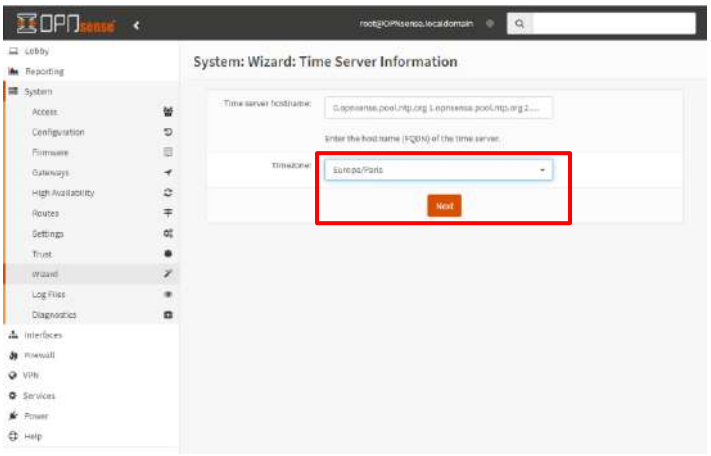
- On arrive au guidage de la configuration. Il faudra cliquer sur « suivant ».



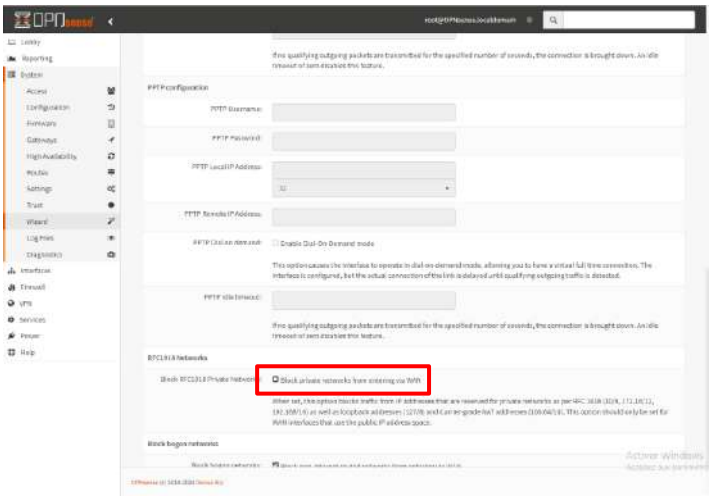
- Ici on change le nom de notre pare-feu par un nom plus parlant les espaces ne sont pas acceptés.

- On définit le domaine de l'école par « iia-laval.info ».

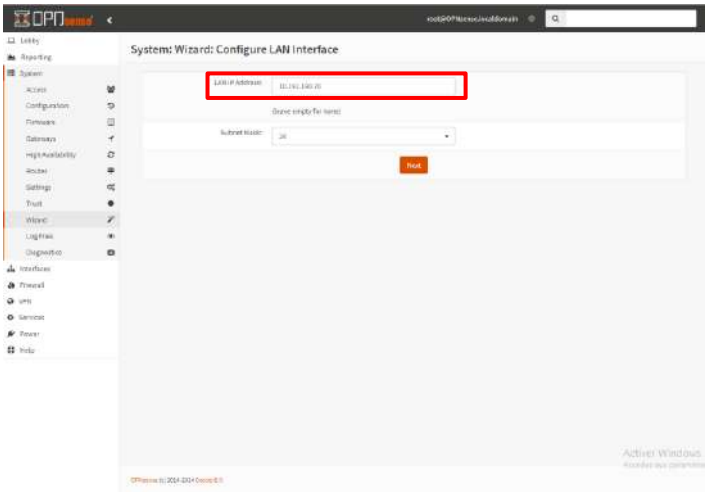
  D'ailleurs ici nous pouvons configurer le DNS secondaire utile en cas de problème avec le primaire.



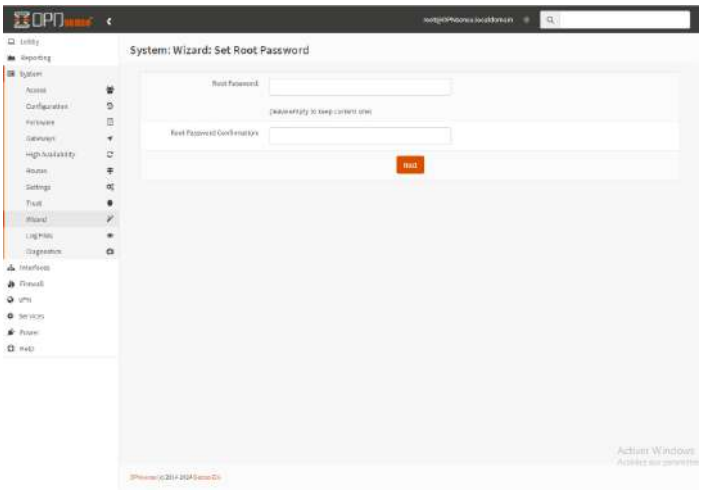
- Selon la zone géographique du serveur il faudra spécifier la capitale du pays en question, si le serveur est situé en France il faudra choisir le « Europe/Paris ».



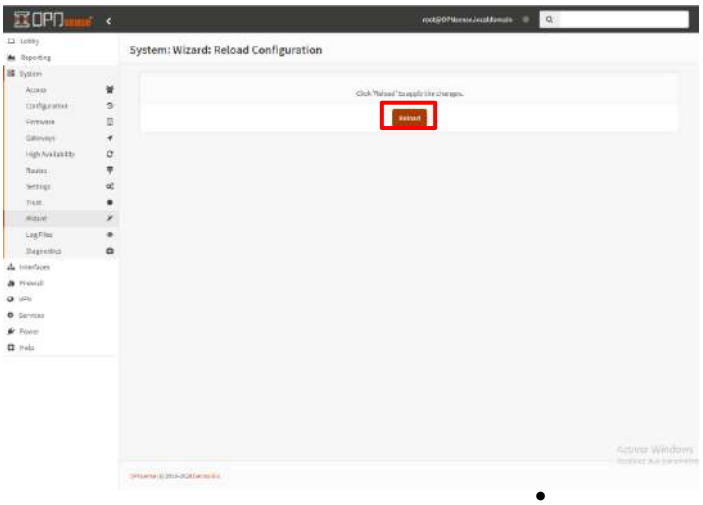
- Enlever la coche « Block private networks from entering via WAN » car le WAN n'est pas directement relié à internet.



- Entrer l'adresse IP de l'interface correspondant au WAN.



- Nous pouvons changer le mot de passe « root » si nécessaire.

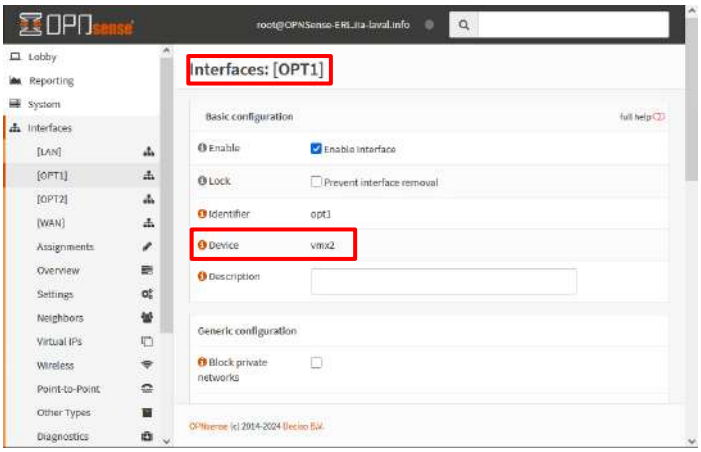


- L'assistant propose le redémarrage du serveur, nous allons accéder à ça demande.

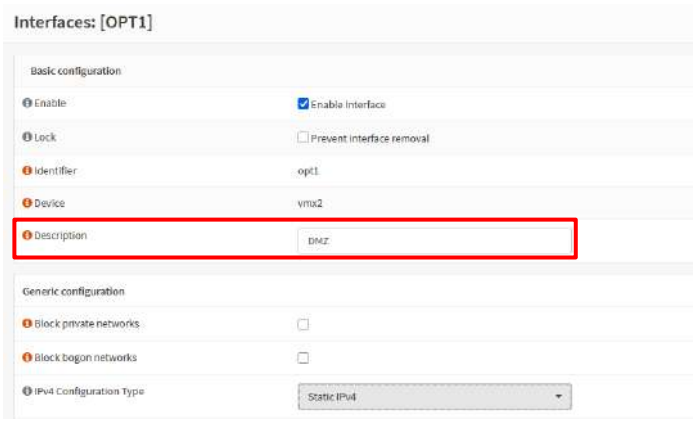


Félicitations ! La configuration initiale est terminée. Entrons dans les détails. Mais avant… Café !

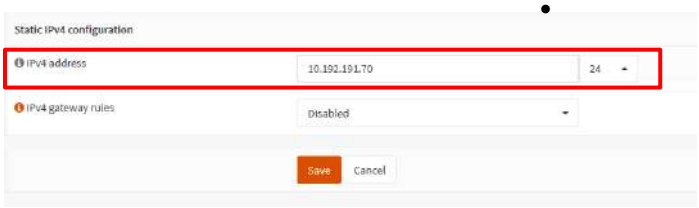
3.5. Définition des interfaces



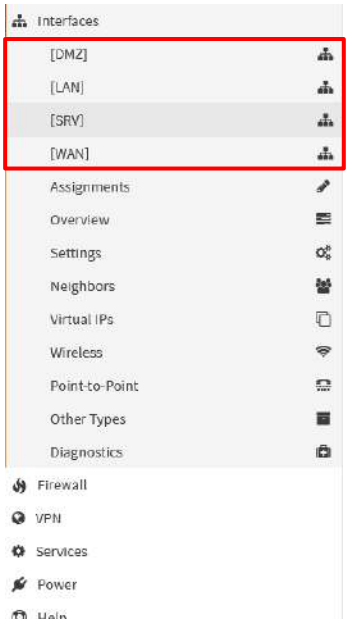
- Il faudra redéfinir les interfaces de manière graphiques.

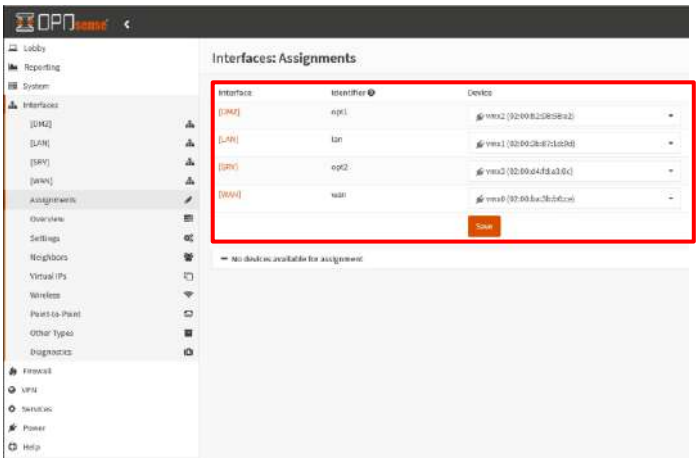


- Il faut se rendre dans « Interfaces » puis sélectionner l'une des interfaces afin de donner une description qui correspondra au nouveau nom de l'interface.

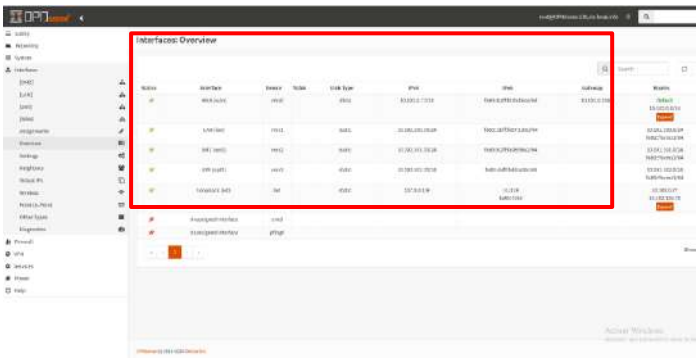


- Définir l'adresse IP de l'interface sélectionner précédemment.



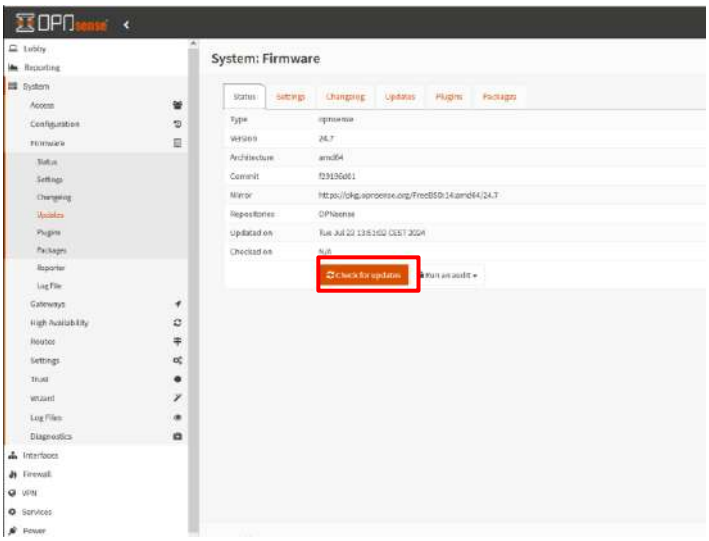


- Voila une vue d'ensemble des assignations de nom. Trouvable dans « interfaces » puis « assignments ».



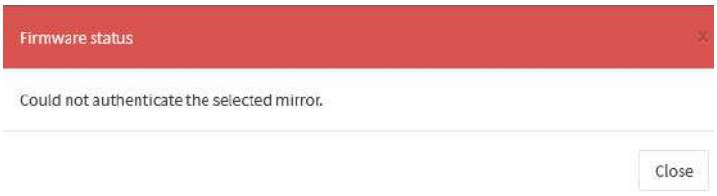
- Voilà une vue d'ensemble plus détaillé. Trouvable dans « Interfaces » puis « Overview ».

3.6. Mise à jour

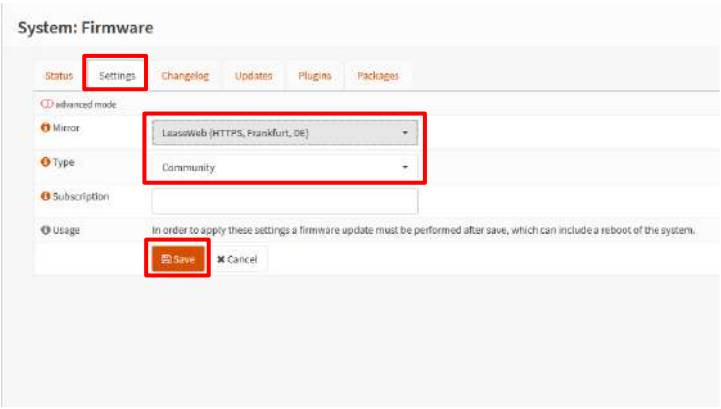


- Dans cette partie on va traiter de mise à jour, pour la sécurité d'une machine il est important de disposer des dernières mises à jour de sécurité notamment.

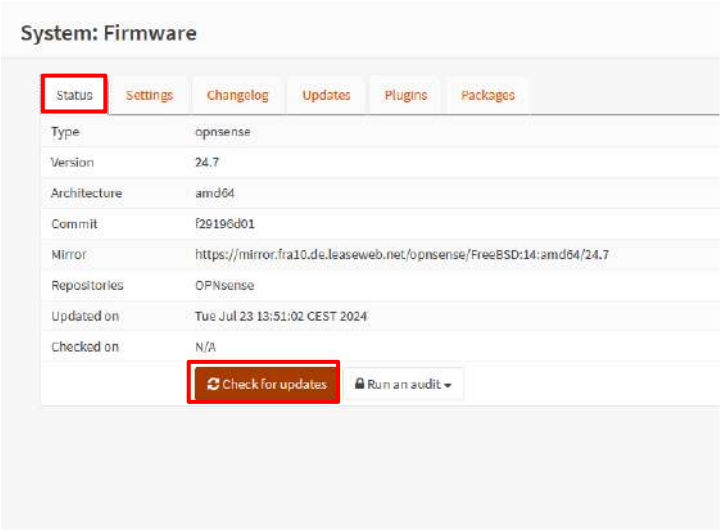
- En se rendant dans « System », « Firmware », « Updates » on a un bouton « Check for updates » afin de vérifier les dernières mises à jour.



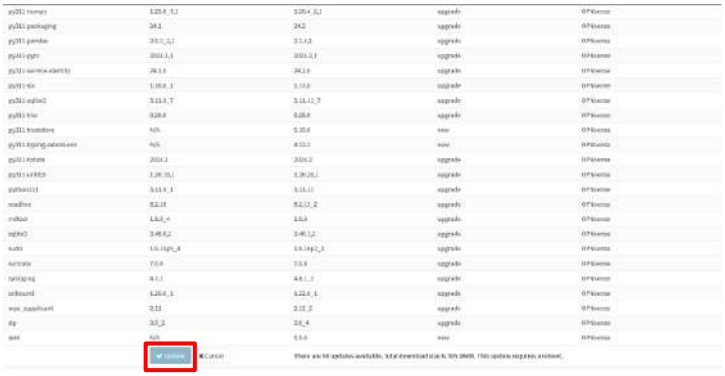
- Cette erreur peut s'afficher dans ce cas.



- Il faudra se rendre dans l'onglet « Settings » en haut choisir un miroir dans la partie « Mirror » de préférence il faut choisir le plus près de son serveur dans mon cas l'Allemagne puis de sauvegarder en cliquant sur « Save ».



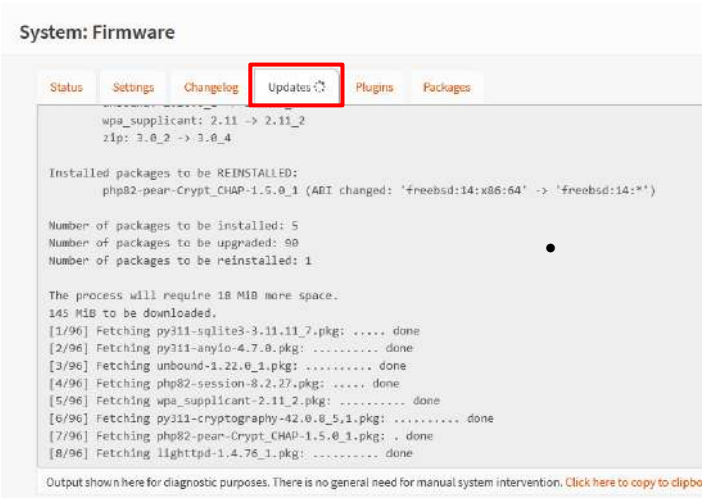
- Retourner dans « Status » afin de revérifier les mises à jour.



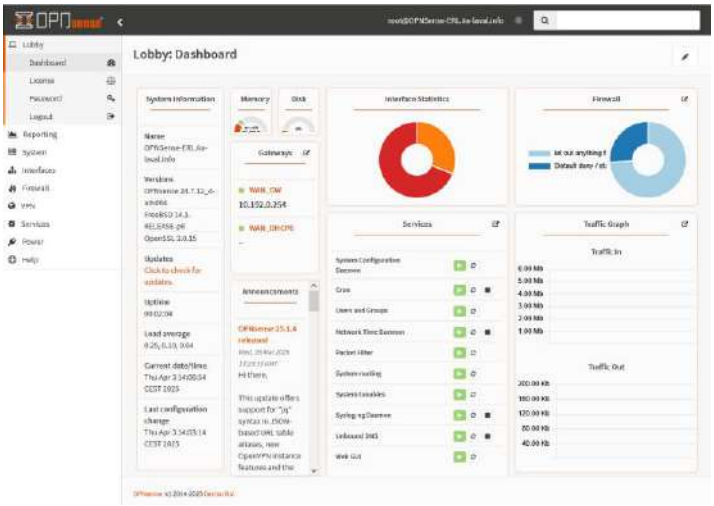
- Les mises à jour trouvé cliquer sur « Update » afin de lancer les mises à jour.



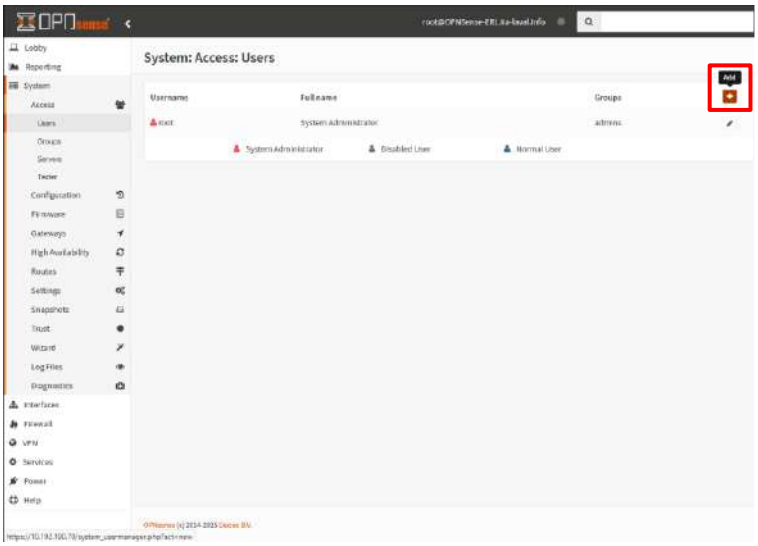
- Un message nous invite à relancer notre pare-feu.



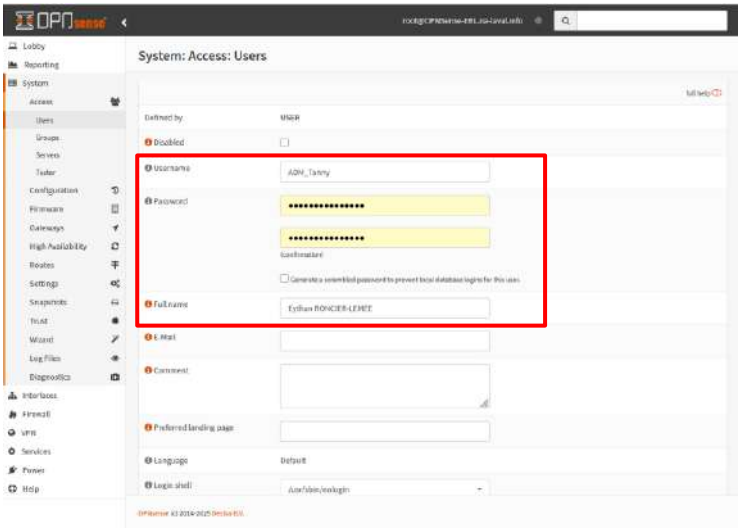
On remarque l'avancement des mises à jour dans l'onglet « Updates ».



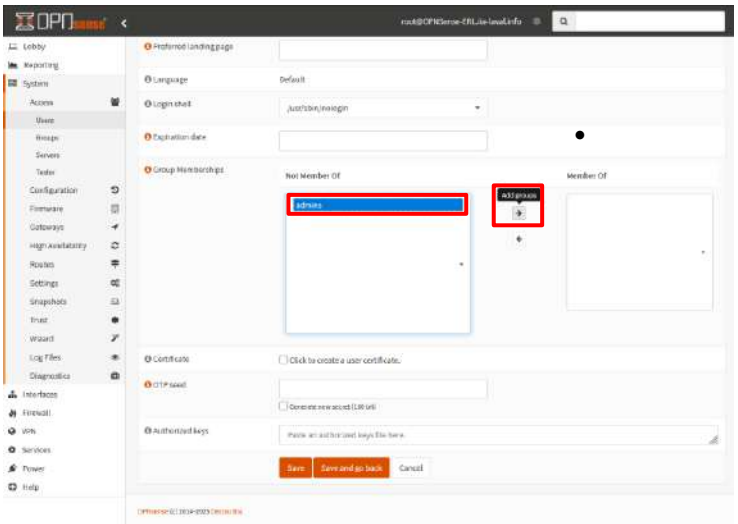
3.7. Gestion utilisateur



- Pour créer un nouvel utilisateur il faut se rendre dans « System », « Access » puis « Users ».
- Le « + » nous permet de créer un nouvel utilisateur.



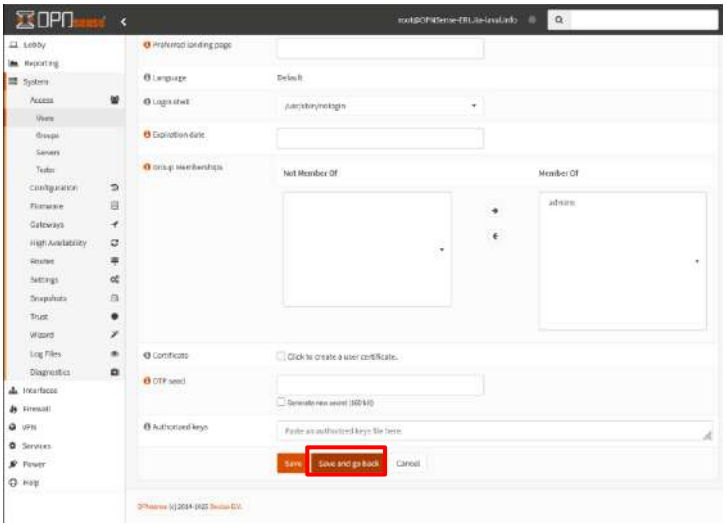
- Ces informations seront demandées :
  - Nom d'utilisateur (Username)
  - Mot de passe (Password)
  - Nom complet (Full name)



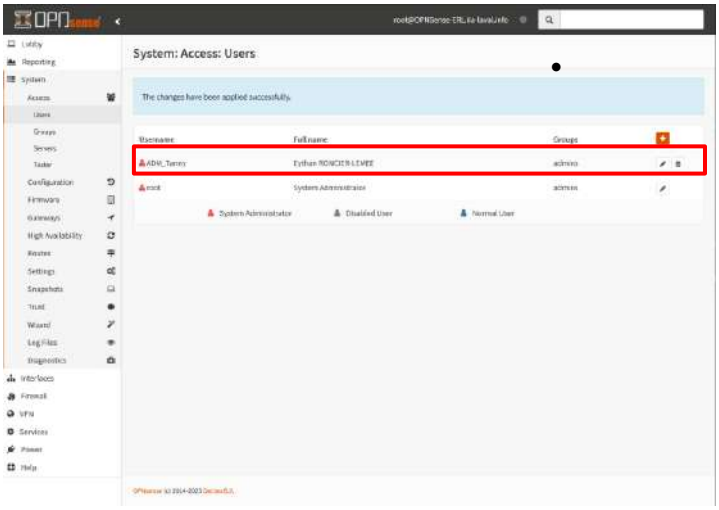
- Si l'on souhaite attribuer à l'utilisateur le rôle administrateur il faudra l'ajouter au groupe dit « admins ».
  Pour se faire dans la partie « Group Memberships », faites un simple clic afin de mettre en surbrillance le groupe que vous souhaiter ajouter puis de cliquer sur la flèche allant à droite pour lui assigner le groupe.



- Le groupe « admins » a bien été assigner à l'utilisateur.



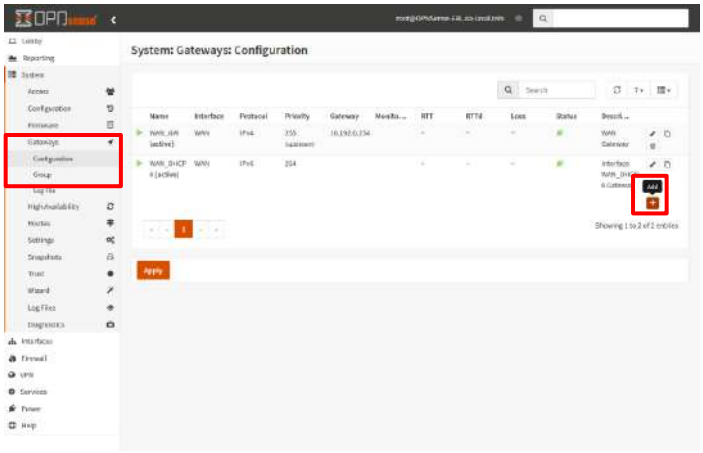
- Les modifications faites il faudra faire « Save and go back » afin de sauvegarder et revenir en arrière.



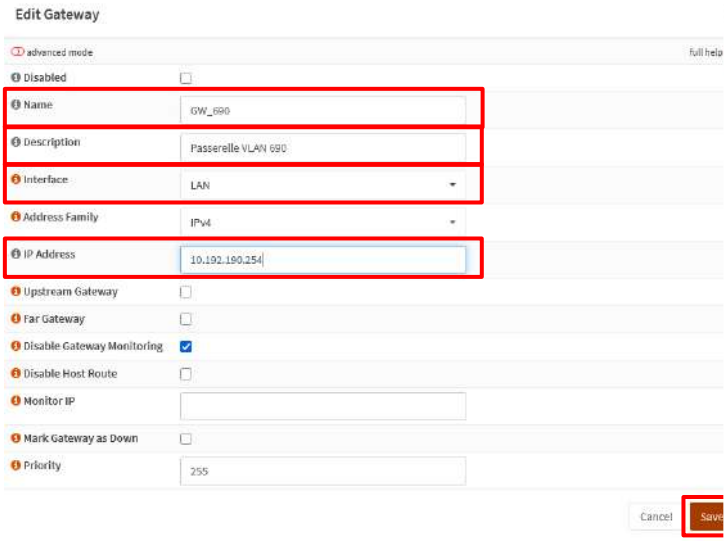
- On remarque que l'utilisateur précédemment créer apparait ici.

3.8. Configuration du pare-feu

3.8.1. Ajout d'une passerelle

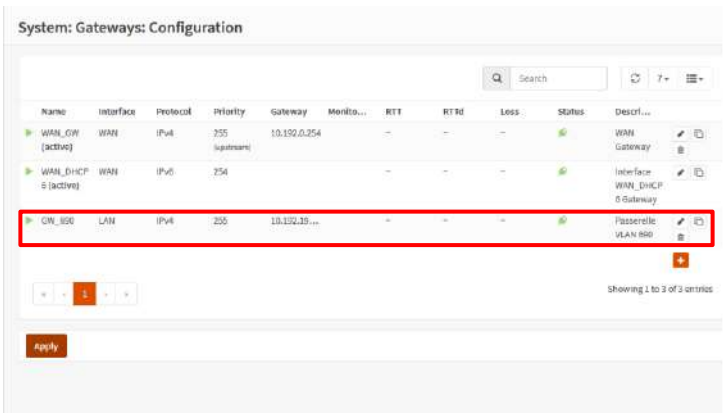


- Afin d'ajouter les passerelles des vlan il faudra se rendre dans « System », « Gateways » puis « Configuration ».
- Comme pour les autres menus l'ajout d'une passerelle se fait via le bouton « + ».



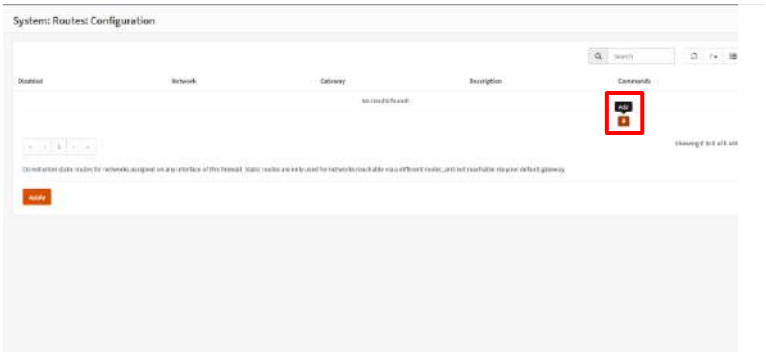
- Il nous sera demander les informations suivantes :
  - Nom (Name)
  - Description
  - Interface
  - Adresse IP (IP Address)

- Enfin il faudra sauvegarder les modifications.

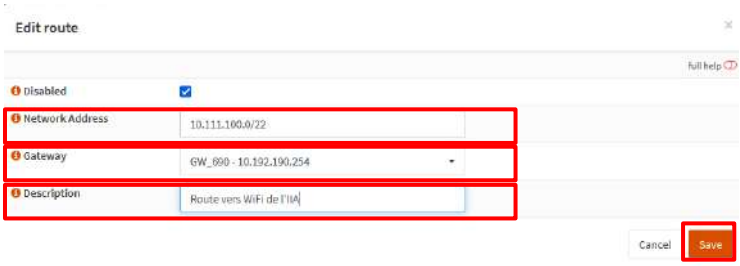


- On remarque qu'elle a bien été ajoutée mais il faudra bien penser à cliquer sur le bouton « Apply » afin d'appliquer les différentes modifications.

3.8.2. Ajout d'une route



- La route est le cœur d'un routeur il permet de choisir la destination d'une requête de façon manuel dans mon cas je vais créer un exemple via le bouton « + », mais le laisser désactiver.



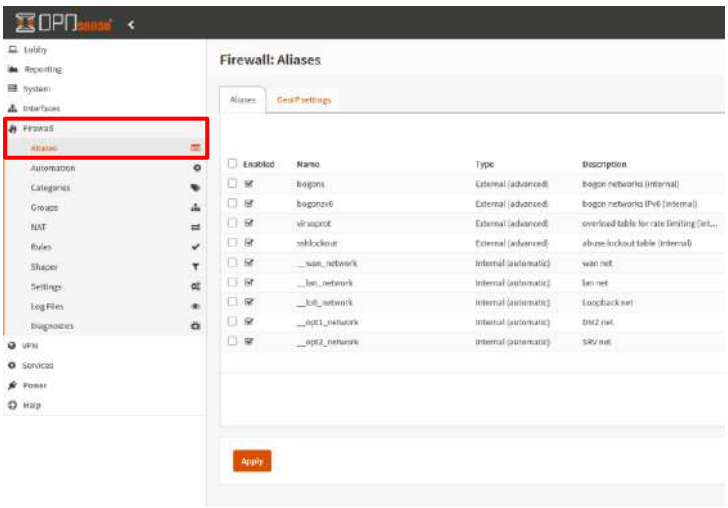
- On nécessite d'avoir ces données afin d'établir une route :
  - Réseau (Network Address)
  - Passerelle (Gateway)
  - Description



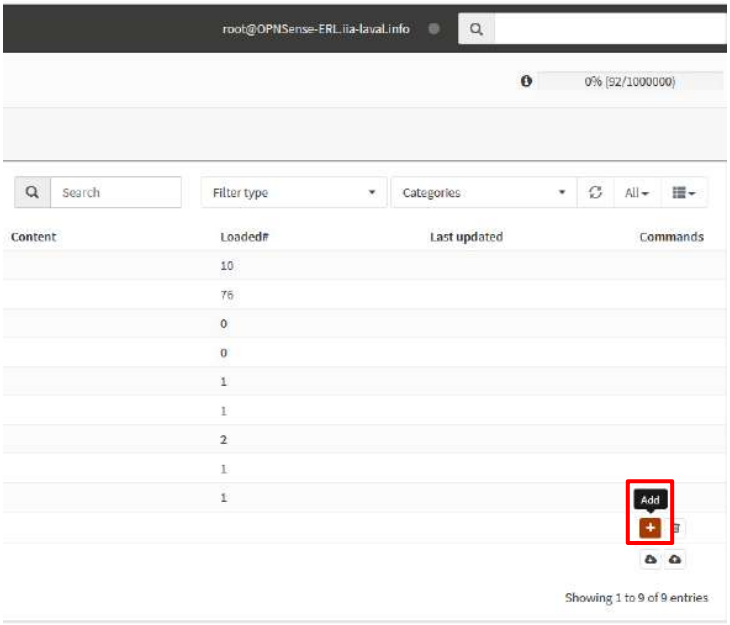
Une fois satisfait on peut cliquer sur « save » puis « apply ».

3.8.3. Ajout d'un alias

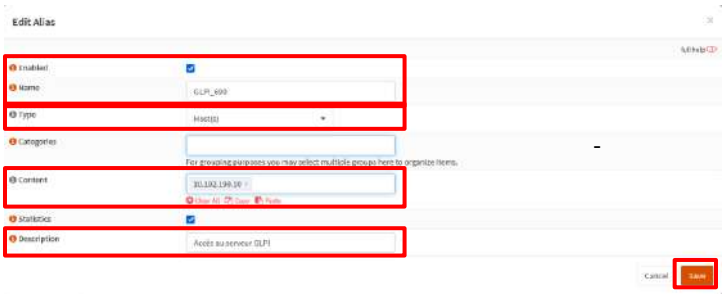
3.8.3.1. Alias pour le serveur GLPI



- Créer un alias se révèle intéressant, un nom court, une adresse, plus simple et plus court bref, meilleur moyen pour retenir ces périphériques.

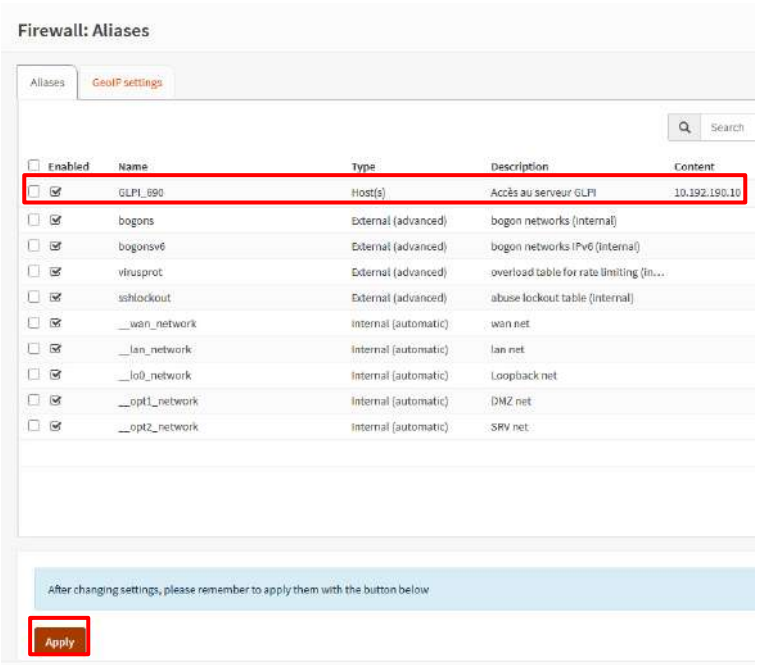


- Créons l'alias du serveur GLPI avec le bouton « + » pour commencer.



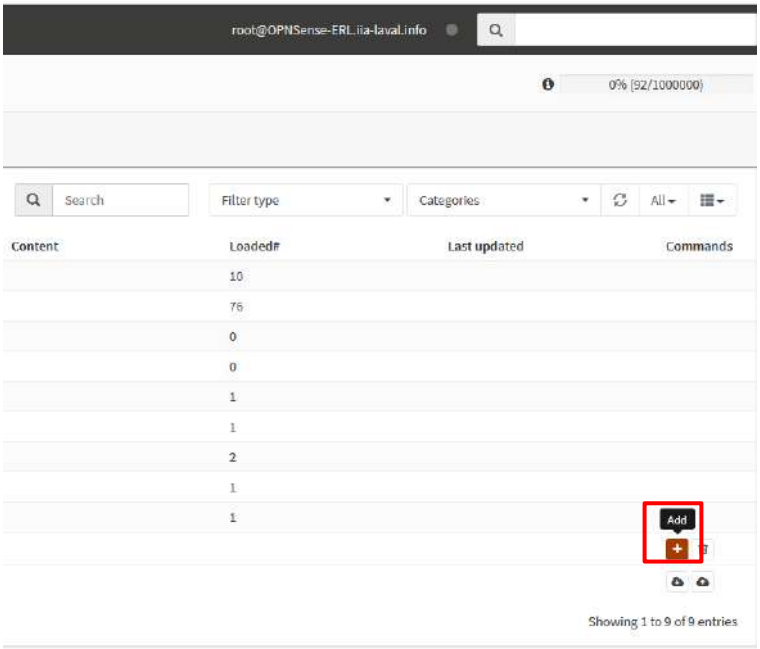
- Nous avons besoin de ces informations :
  - Activé ? (Enabled)
  - Nom (Name)
  - Type de périphérique
  - L'adresse IP (Content)

  Description

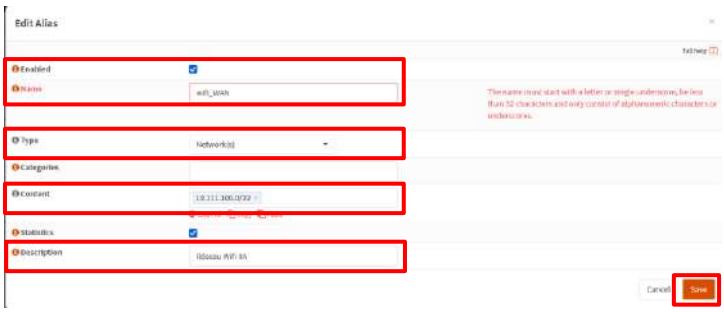


- On remarque que l'alias a bien été créer. Il faudra penser à cliquer sur « Apply » pour appliquer les changements.

3.8.3.2. *Ajout d'un alias pour le réseau Wi-Fi de l'école*

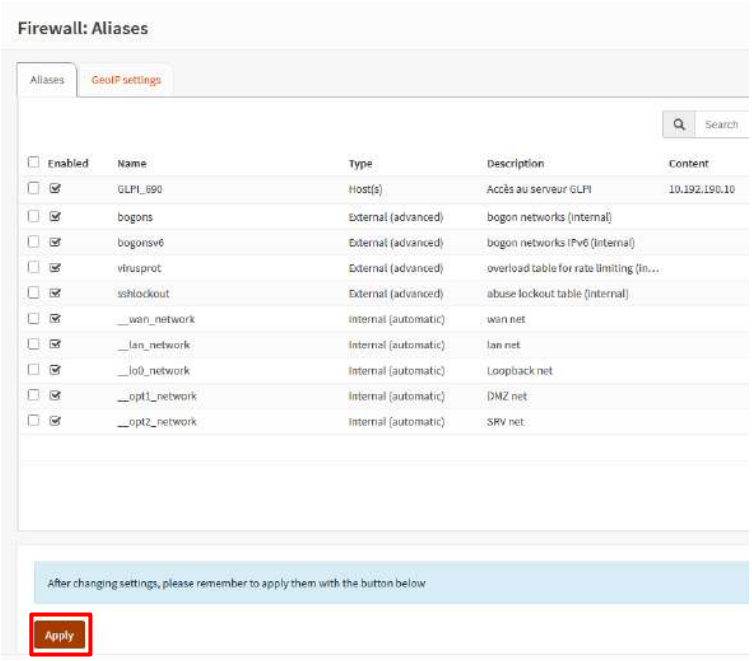


- Créons l'alias du réseau Wi-Fi de l'école avec le bouton « + » pour commencer.



- Nous avons besoin de ces informations :
  - Activé ? (Enabled)
  - Nom (Name)
  - Type de périphérique
  - L'adresse IP (Content)
  - Description

- Il est recommandé d'y ajouter les routeurs et d'y mentionner le VLAN ou le réseau dans le nom de celui-ci afin de s'y retrouver.

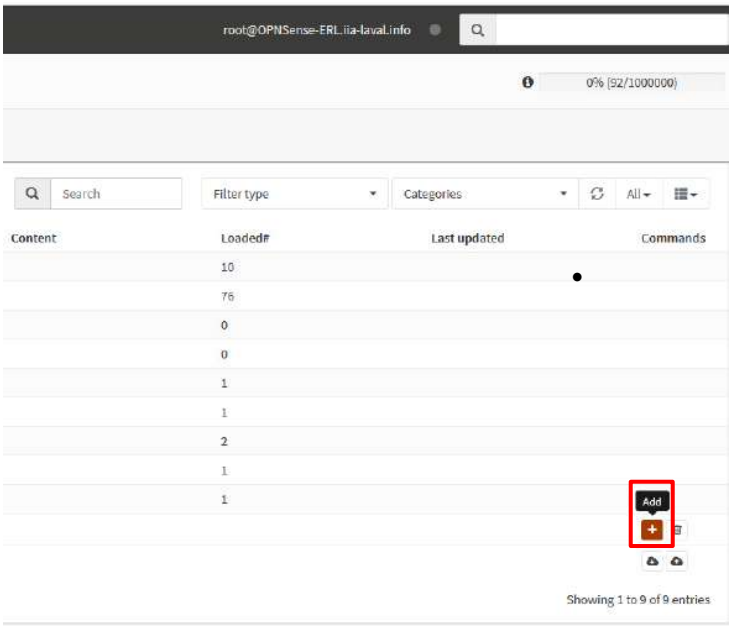


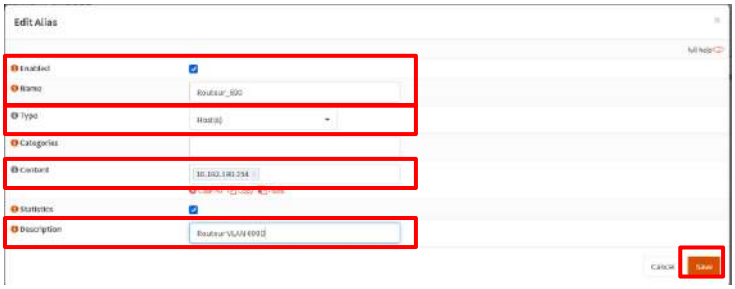
- Lorsque la machine passe en état « RUNNING » c'est qu'elle est en fonctionnement de ce fait l'écran s'affiche sur la ligne supérieur cliquer dessus fera apparaitre « **VMRC** », qui nous sera utile pour la supervision.

- L'avantage avec ce système c'est qu'on n'a pas besoin de le configurer ou du moins beaucoup moins qu'un système classique installé via une image.

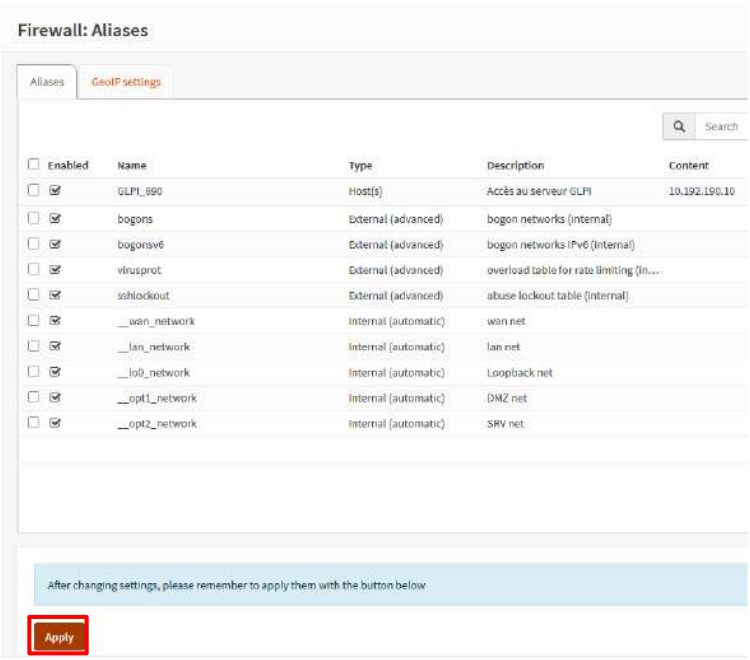
- L'utilisateur est « adminlocal », le mot de passe est « Not24get ».

3.8.3.3. *Ajout d'un alias pour les routeurs*





Afin de reconnaître la machine il est nécessaire de la renommer Pour ce faire il faut se rendre dans le menu Windows puis cliquer sur paramètres ou effectuer la combinaison Windows + i.

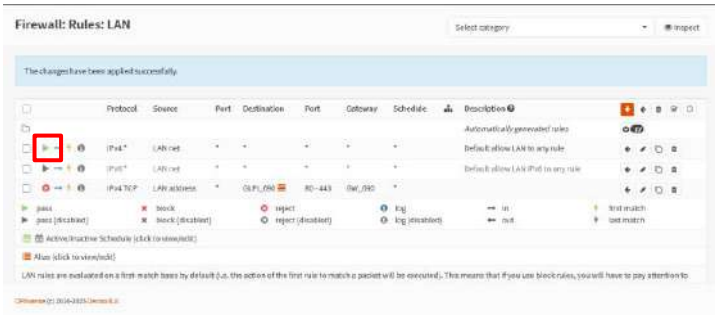


- On remarque que l'alias a bien été créer. Il faudra penser à cliquer sur « Apply » pour appliquer les changements.

3.8.4. Gestion des règles du pare-feu



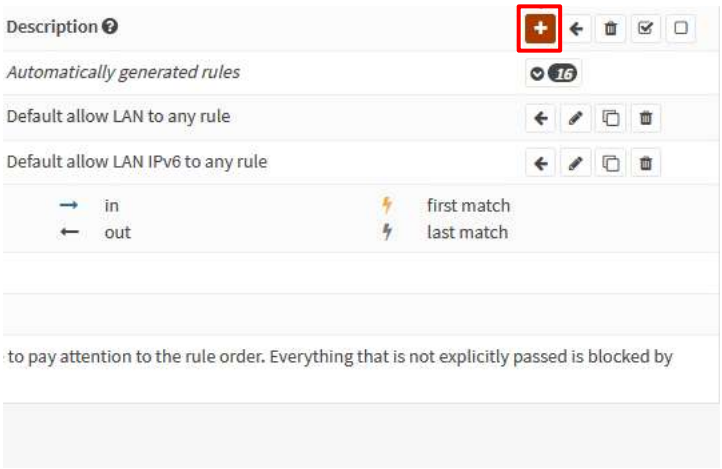
- Désormais on va pouvoir ajouter des règles afin de restreindre des accès ou au contraire de les autoriser.
- Se rendre dans « Firewall », « LAN » ou autres sections de votre réseau.



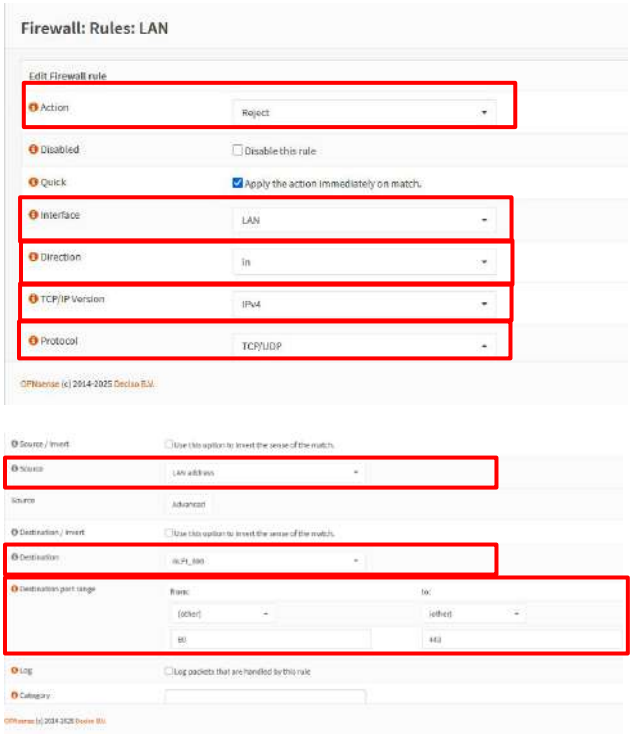
- Pour commencer on va cliquer sur le triangle vert de la règle IPv6 afin de la désactiver et laisser pour le moment le triangle vert entouré en rouge.

3.8.4.1. Contexte 1

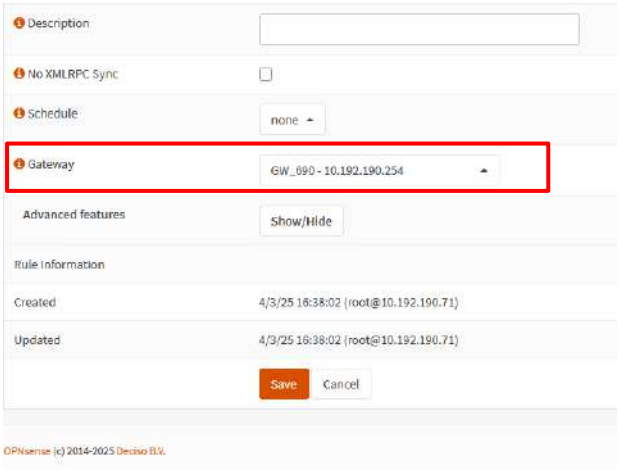
Le but est de bloqué l'accès à la page GLPI au VLAN 690 depuis celui-ci, exemple la console ne peut pas accéder aux ports 80 et 443 du serveur GLPI mais peut envoyer des requêtes en ICMP.



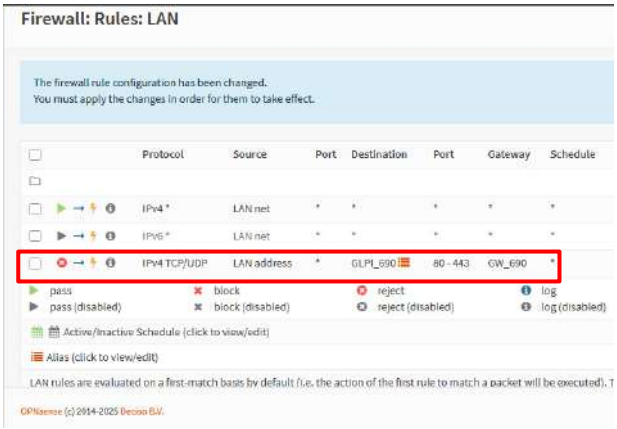
- Cliquer sur le « + » afin d'ajouter une nouvelle règle.



- Ont choisi le type de règle à instauré dans mon cas je souhaite rejeter les requêtes correspondant à mon contexte.
- Choisir sur quelle interface cette règles va s'appliquer (Interface).
- La direction de la requête « in » correspond à une requête vers la destination et « out » depuis la destination.
- Le protocole va correspondre à la norme de transport de la requête dans mon cas :
  - Http comme https utilisent le transport TCP et UDP
  - Mais http utilise le port 80 et https utilise le port 443
- Ont choisi la source et la destination de la requête.
  On peut ensuite choisir les ports à bloquer.



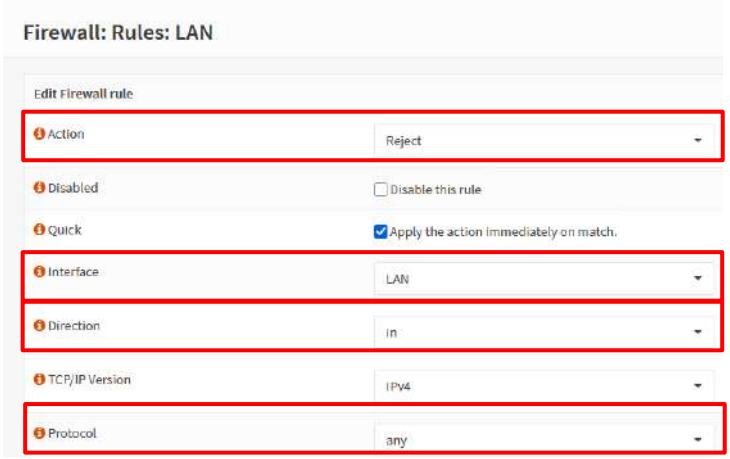
- Ont choisi la passerelle de passage de la requête.



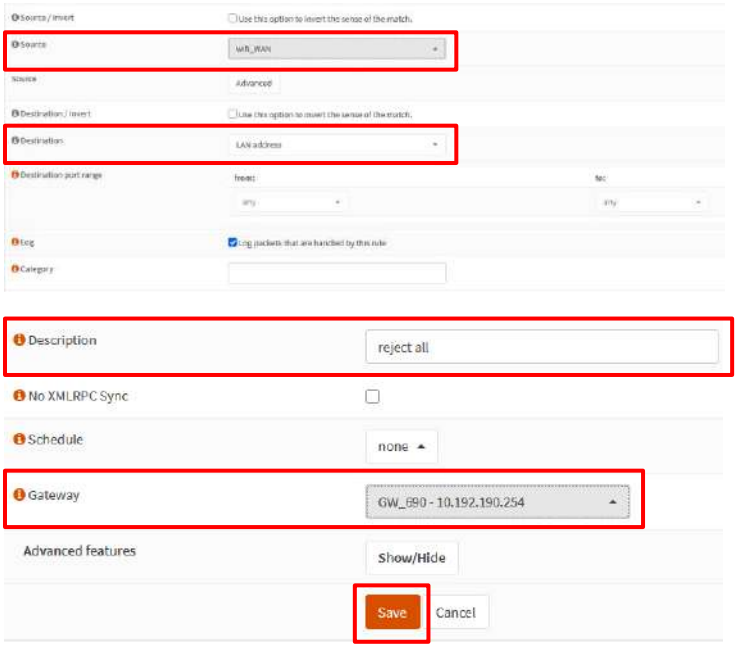
- Puis il faudra sauvegarder en oubliant pas d'appliquer.

3.8.4.2. Contexte 2

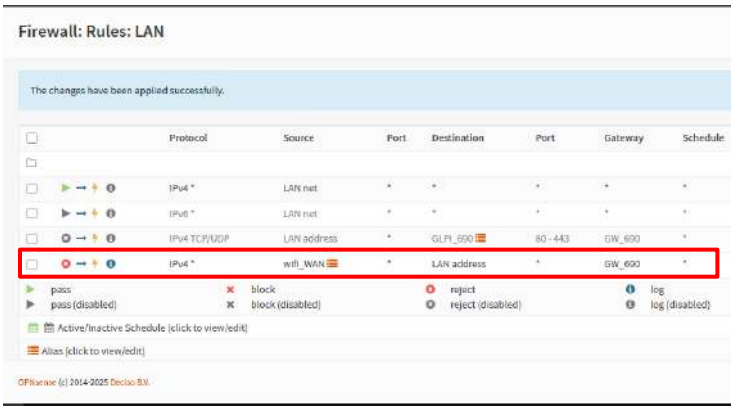
Bloquer l'accès à la partie LAN du réseau part le Wi-Fi de l'IIA.



- Cliquer sur le « + » afin d'ajouter une nouvelle règle.
- Pour bloquer l'accès à la partie LAN du réseau par le WiFi de l'école il faudra créer une règle « Reject ».
  Etablir la même méthodologie que le premier contexte pour l'établissement de la règle.

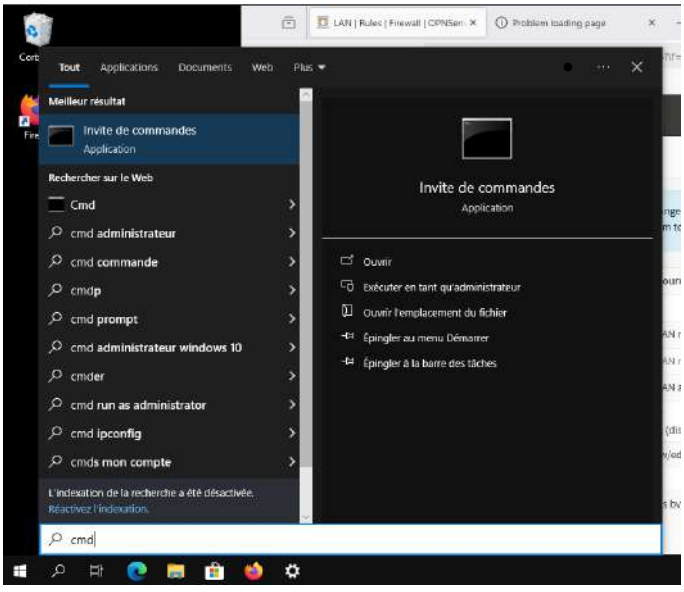


- On choisit donc l'interface, la direction, le protocole, la source, la destination, une description, la passerelle et enfin on sauvegarde.

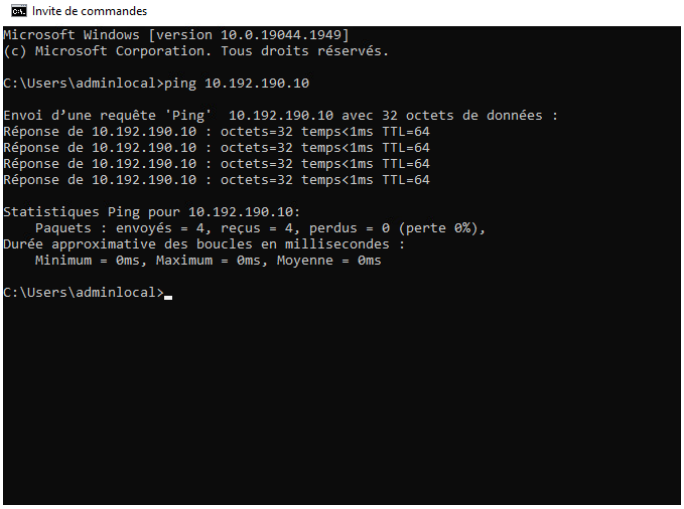


- On remarque les deux règles créer et une légende figure en dessous des règles pour signifier l'état.

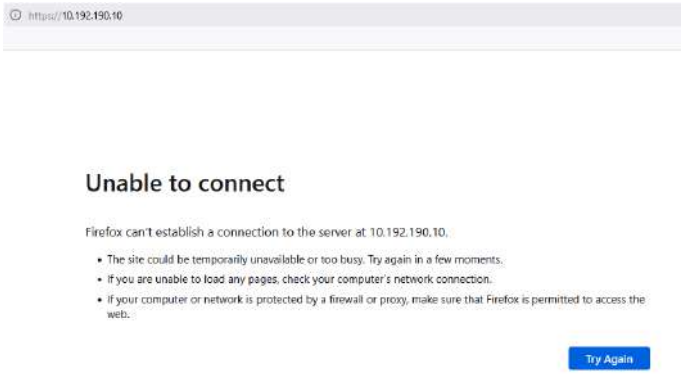
3.8.5. Test de la règle du contexte 1



- Pour tester ma règle concernant le serveur GLPI je vais utiliser la console.
  Je me rends dans l'invite de commande afin d'y faire plusieurs commandes.



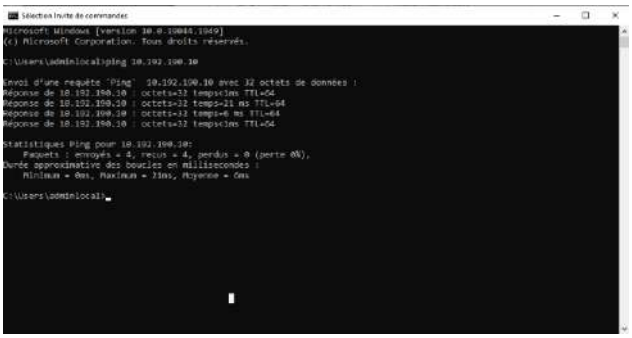
- La première commande me sert à tester que le serveur GLPI est joignable on remarque que oui.



- Toutefois la règle fonctionne puisque le navigateur ne parvient pas à l'atteindre.



- Pour vérifier qu'il ne s'agit pas d'un problème de mon navigateur je désactive la règle que je viens d'établir.



Je refais le test de joignabilité et m'assure que le serveur est toujours joignable malgré ma modification.



En retournant dans mon navigateur lorsque j'actualise la page. On me demande un nom d'utilisateur et un mot de passe pour mon compte GLPI. Ma règle est donc fonctionnelle.

3.9. Commandes Supplémentaires

Permet de désactiver le PARE-FEU

```
Pfctl –d
```

Permet d'activer le PARE-FEU

```
Pfctl –e
```