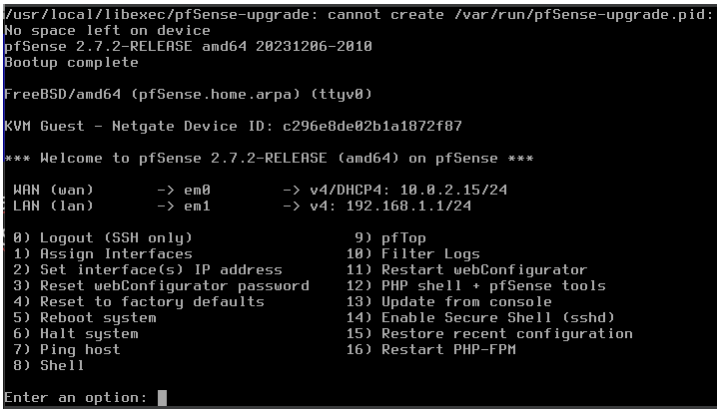
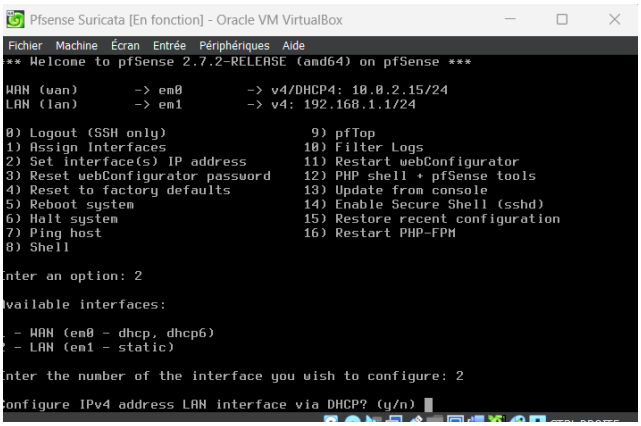
Procédure de configurations PfSense :

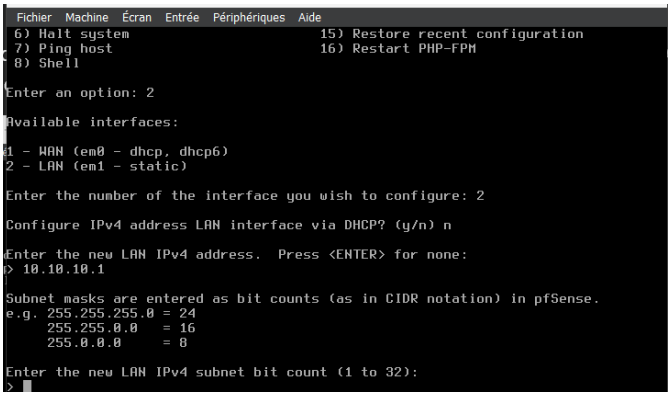
On peut voir que notre interface WAN a une adresse IP attribuez automatiquement via DHCP et que notre interface LAN a une adresse par défaut 192.168.1.1 nous allons configurez tous cela pour quelle soit en accords avec notre schéma d'infrastructure :



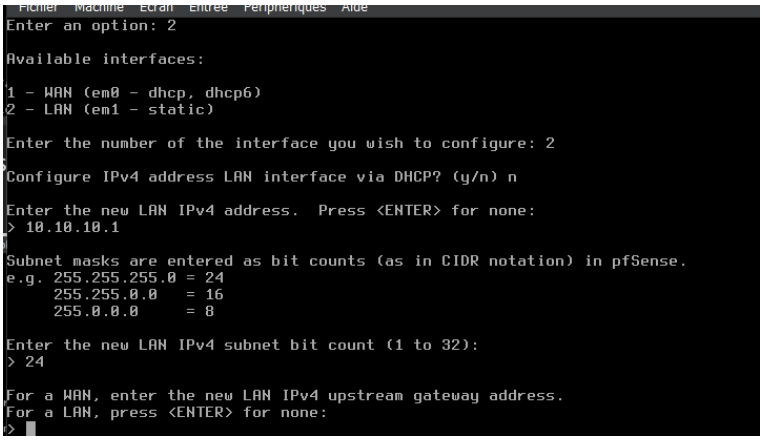
On veut rétribuer notre interface LAN donc on rentre l'options 2 puis on sélectionne notre LAN en rentrant l'options 2 également :



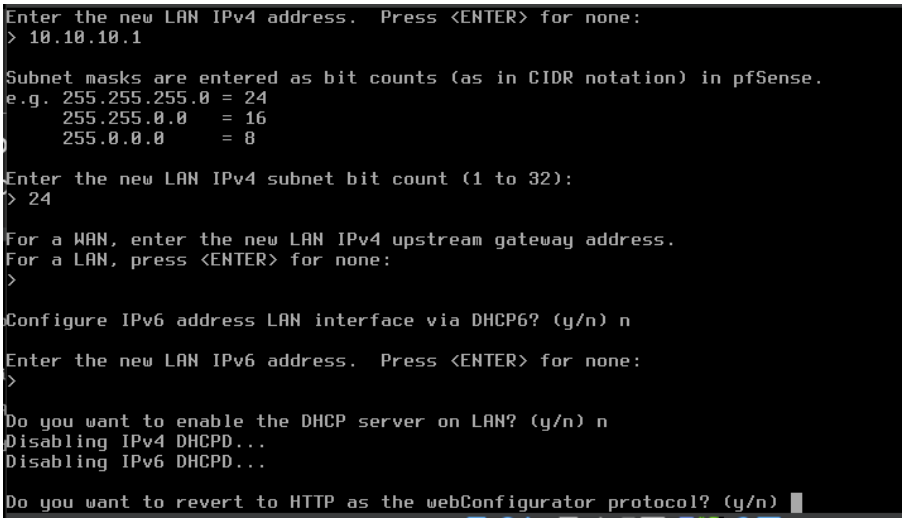
On ne configure pas l'interface via DHCP donc on ecrit n pui s Entrez et on écrit l'adresse ip de notr LAN 10.10.10.1 :



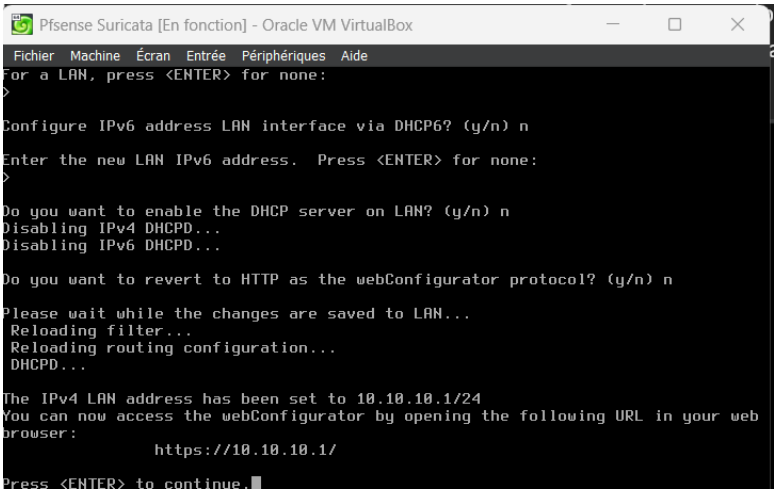
Notre masque de sous reseaux est 255.255.255.0 en notation CIDR c'est /24 on écrit donc 24 dans l'invite de commande :



On n'a pas besoins de mettre un WAN en presse Enter, on ne vas pas configurez le DHCP6 donc on sélectionne n, on ne veut pas non plus d'adresse IPv6 donc on presse ENTER et on ne veut pas configurez le DHCP donc on sélectionne « n » et entrez :

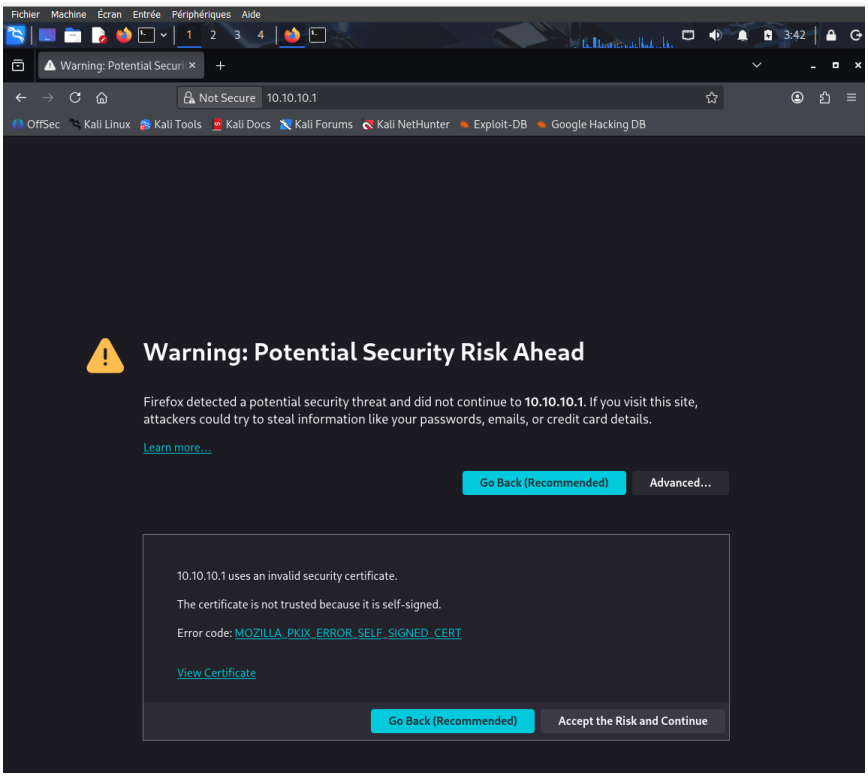


On ne veut pas non plus configurez http on le laisse en HTTPS, on n'arrive ensuite sur le récapitulatif nous indiquant que pfsense et accessible à l'adresse https://10.10.10.1 on appuis sur Entrez pour continuer .

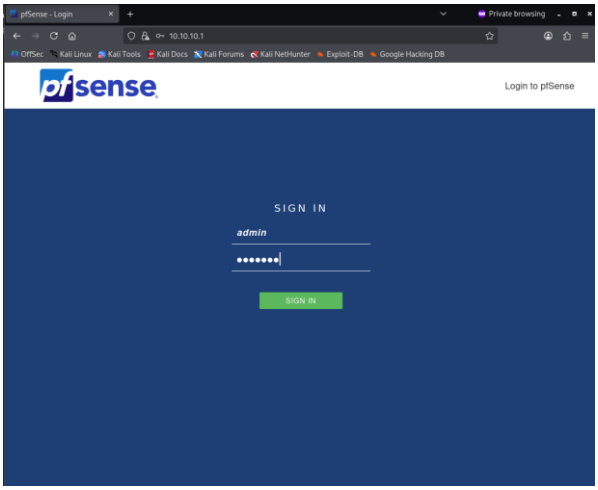


On se rend sur une machine client dans notre réseau qu'on n'aura préalablement préparez et mis dans le LAN (Sinon suivait la procédure Client) on accède à Pfsense via le navigateur de notre Client :

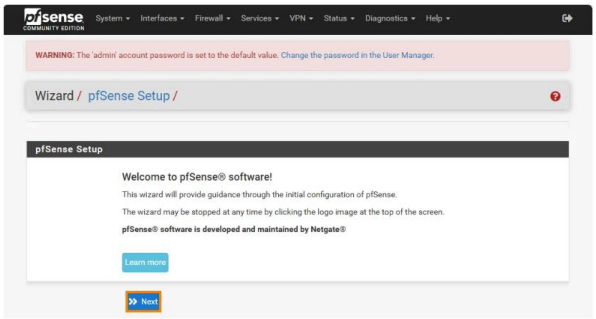
Sélectionner « Advanced » puis « Accept the Risk and Continue »



Vous arriver sur cette page les identifiants sont « admin » et « pfsense » :



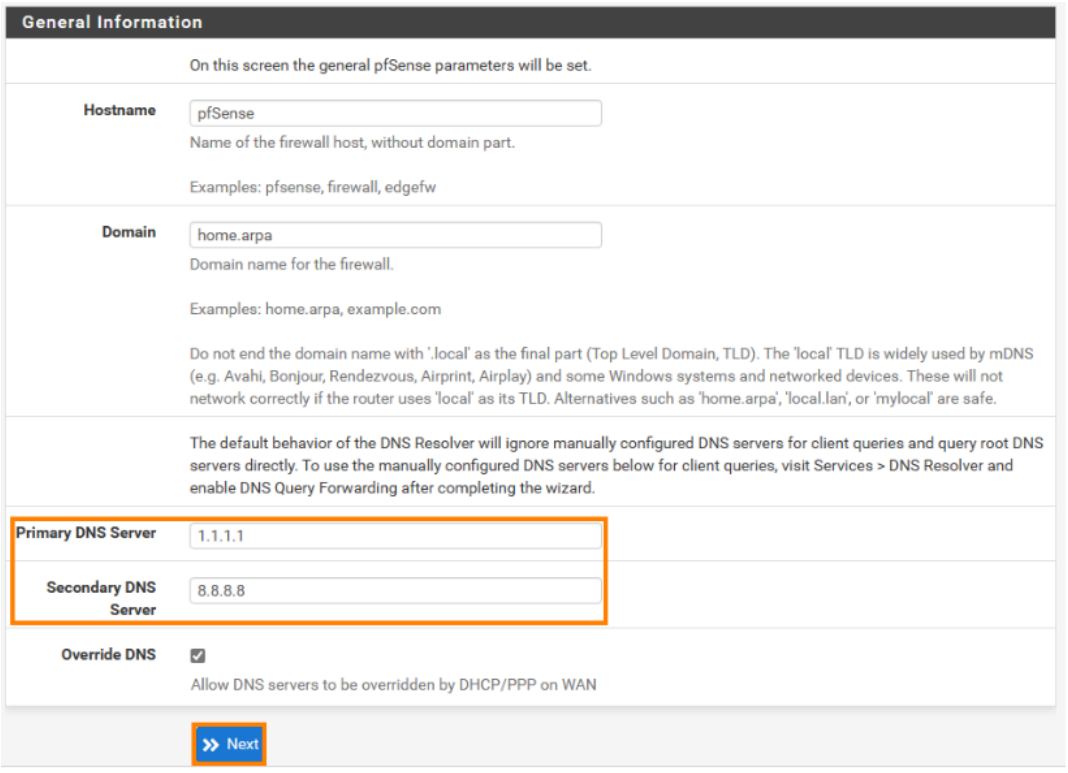
On arrive sur l'assistant de configuration Web. Cliquer sur Next :



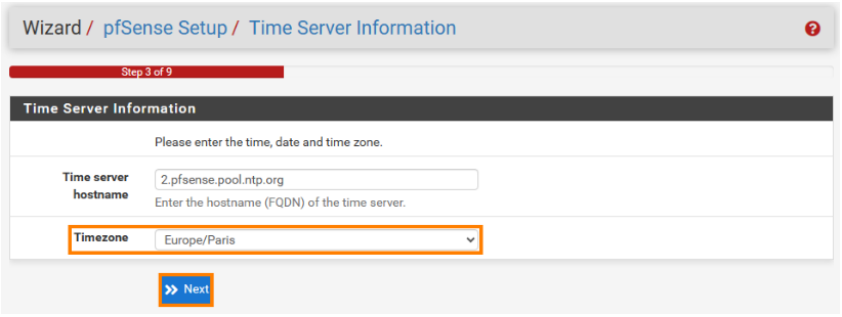
Cliquez à nouveau sur "**Next**" pour valider les modalités de support fourni par l'éditeur.



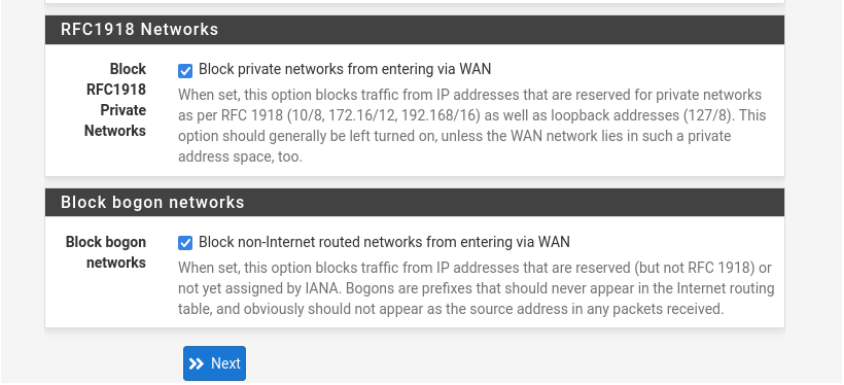
Ici on va mettre nos adresse DNS par défaut 1.1.1.1 et 8.8.8.8 vous pouvez adaptez si vous le voulez a savoir qu'on le changera par la suite car nous créeront notre propre serveur DNS.



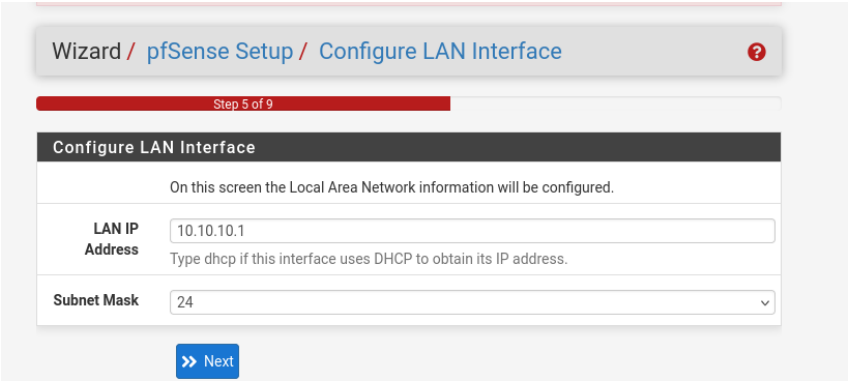
On configure le fuseau horaire pour notre emplacement important pour avoir des logs a jour.



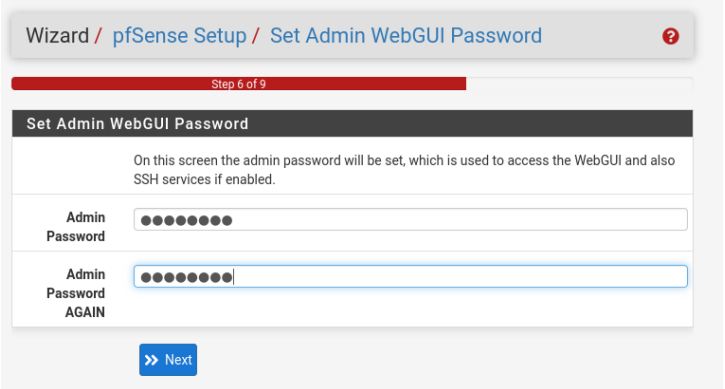
On arrive sur la configuration de l'interface WAN qui est déjà automatiquement configuré via le NAT donc pas besoins de le configuré on descend jusqu'en bas et on fait Next.



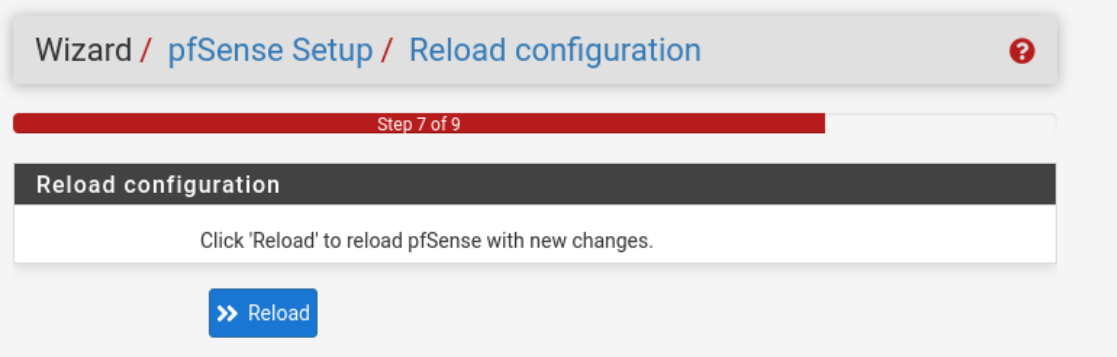
Notre LAN que nous avons déjà configuré donc Next :



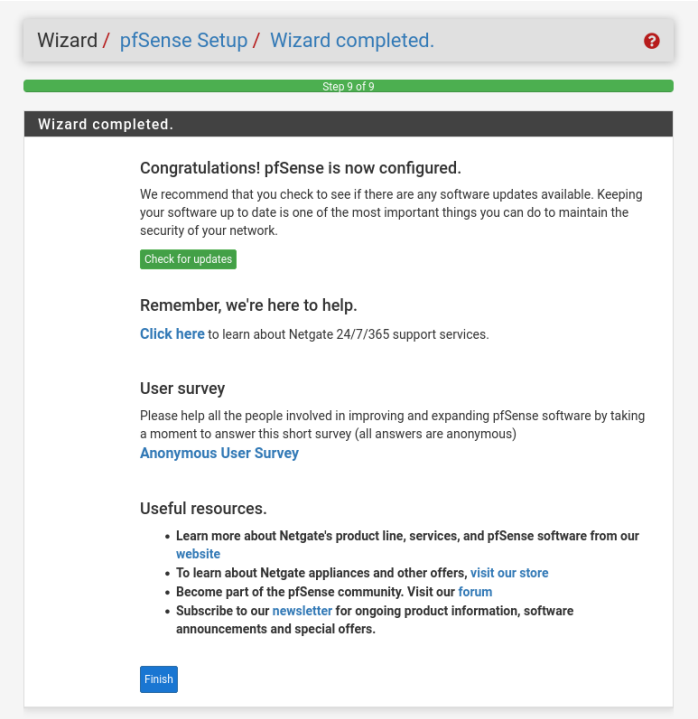
On change le mdp par défaut par un mdp robuste. Dans la suite de la procédure on désactivera le compte admin pour le remplacer par un compte qui est propre à notre entreprise.



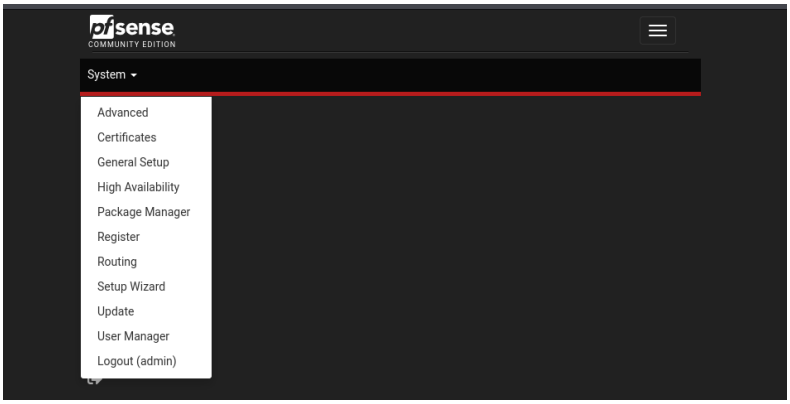
On Reload :



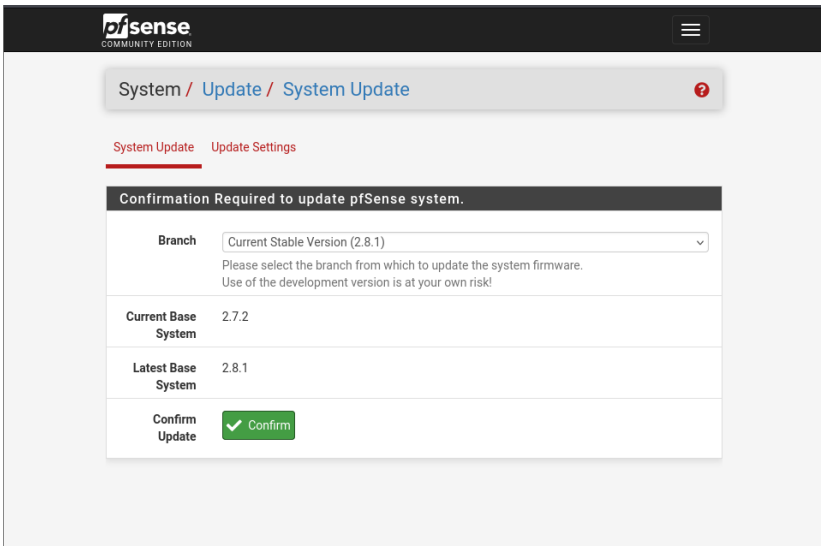
On clique sur Finish pour terminer la conf de base de PfSense :



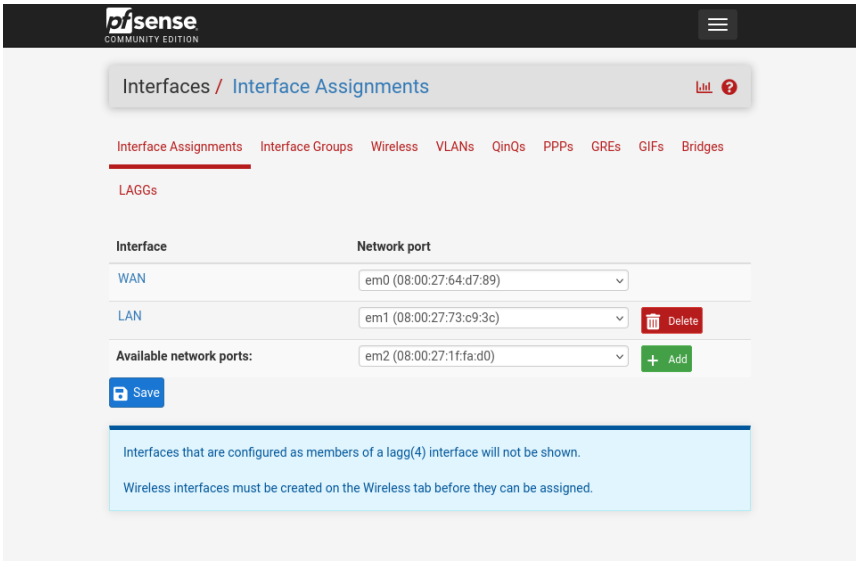
N’hésiter pas a aller dans System puis Update pour vérifier si vous êtes bien ajour.



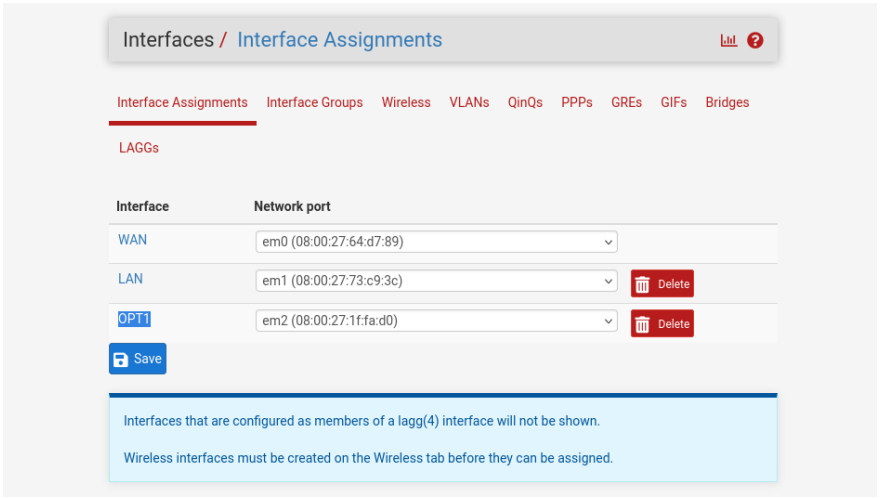
Sinon m'était à jour votre PfSense :



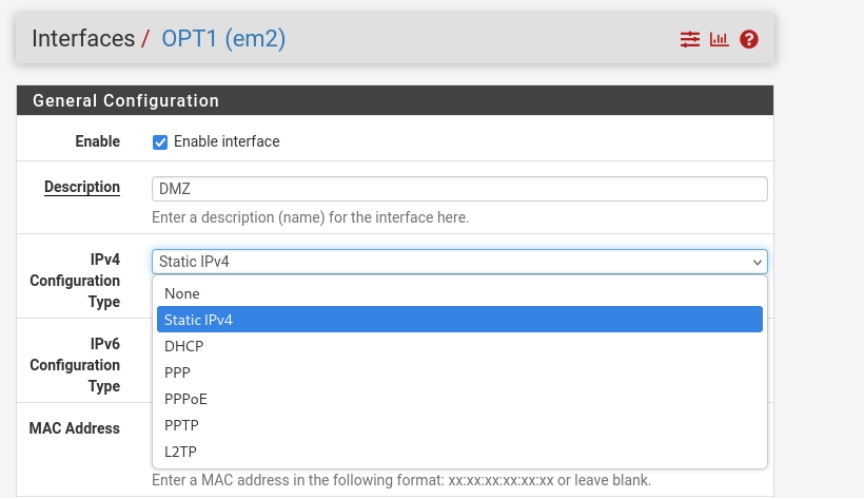
On vas maintenant assigner notre Interface a notre DMZ rdv dans Interfaces > Assignement :



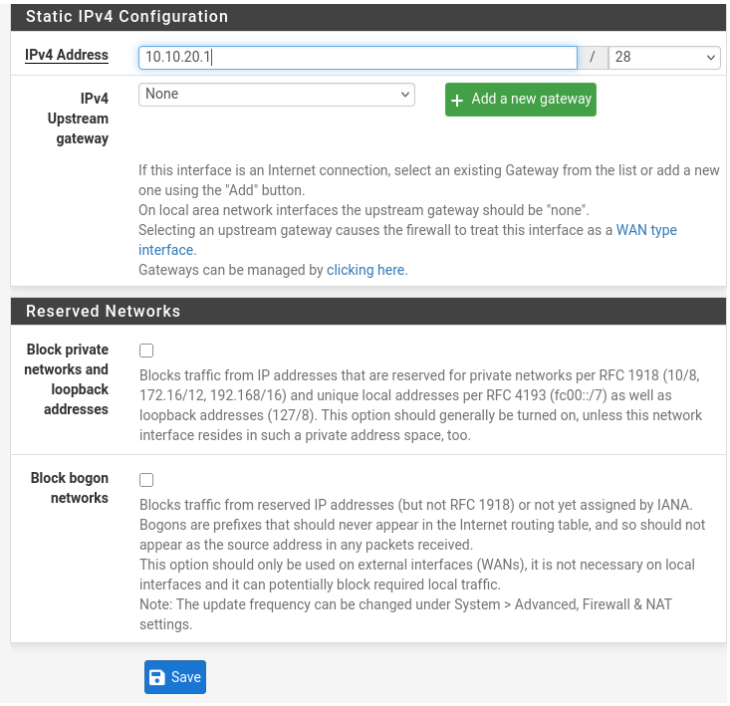
On clique sur Add et cliquez sur OPT1



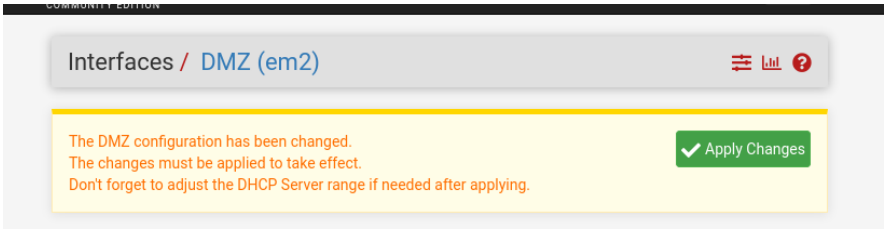
On sélectionne « Enable Interface », on la renomme DMZ, Dans « IPv4 Configuration Type » on sélectionne « Static » dans le menu déroulant :



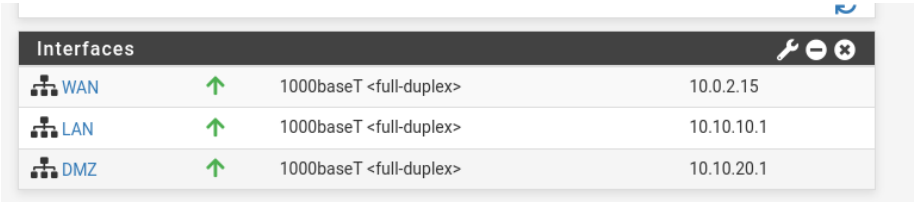
On ajoute notre adresse ip conformément a notre shéma puis on clique sur « Save » :



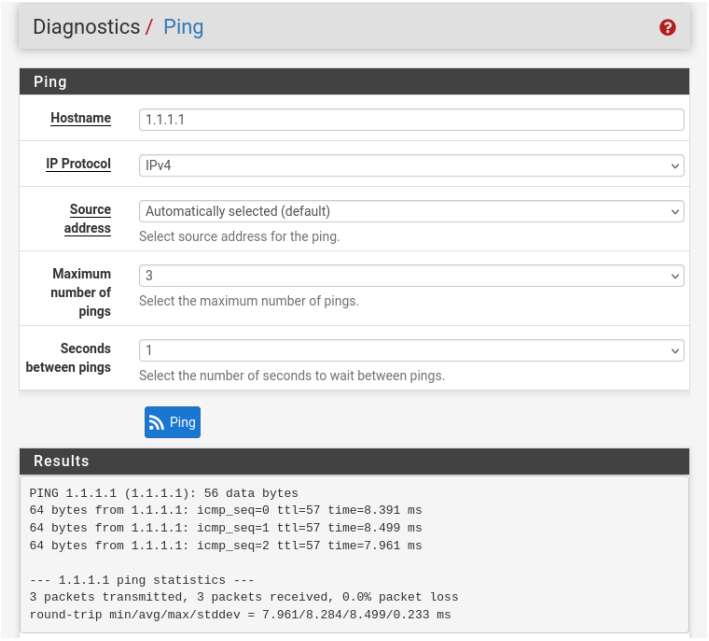
Et sur « Apply Change » :



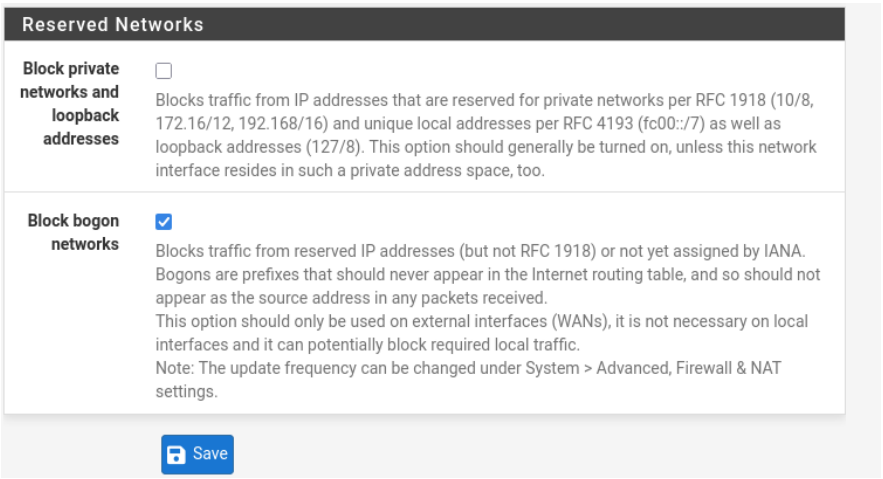
On peut voir dans notre tableau de bord que toute nos interfaces son bien UP :



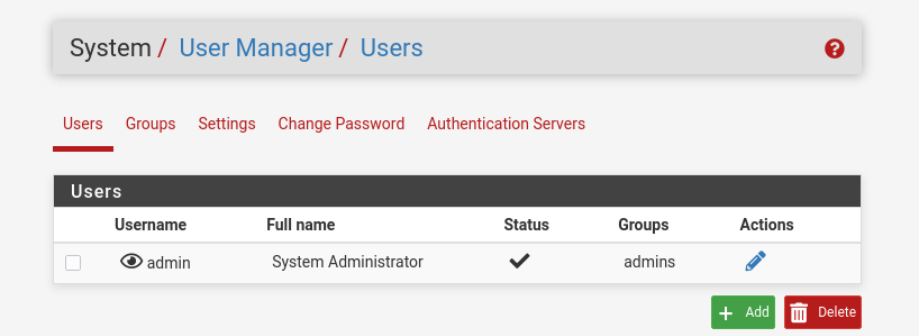
Tester si vous avez bien accer a internet avec un ping d'un DNS public comme 1.1.1.1, rdv dans Diagnostic > Ping :



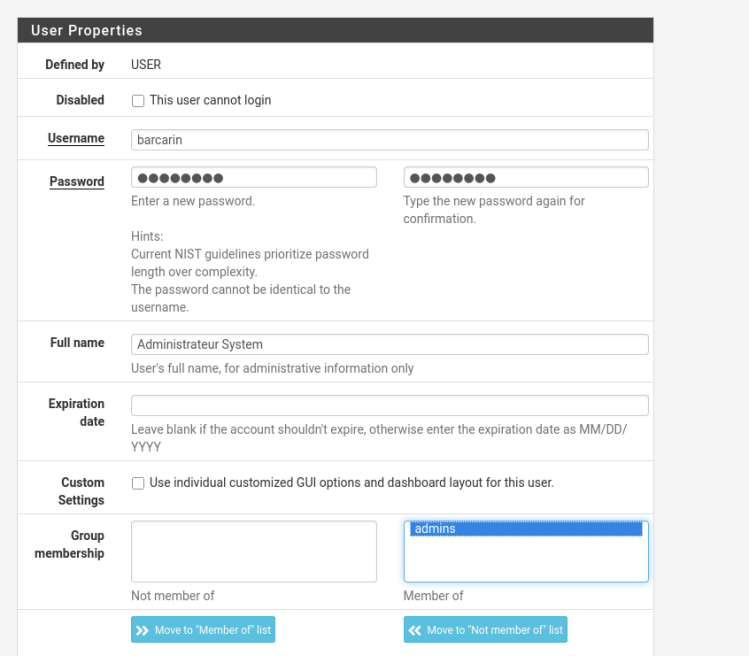
Si le Ping Echoue RDV dans Interface > WAN descendez tout en bas est décochez « Block private networks and loopback adresses » Save puis Apply redémarrez la VM Pfsense puis retestez. :



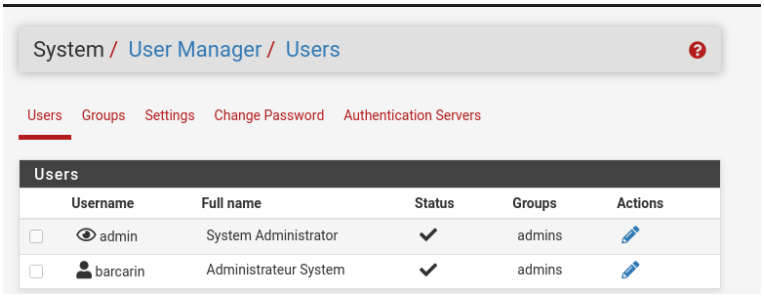
Nous allons créer notre Propre utilisateur rdv dans System > User Manager



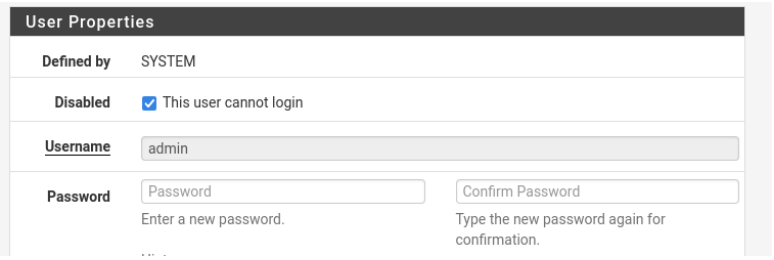
Nous mettons le nom de notre entreprise un mdp robuste et on l'ajoute au groupe « admins » puis « Save » :



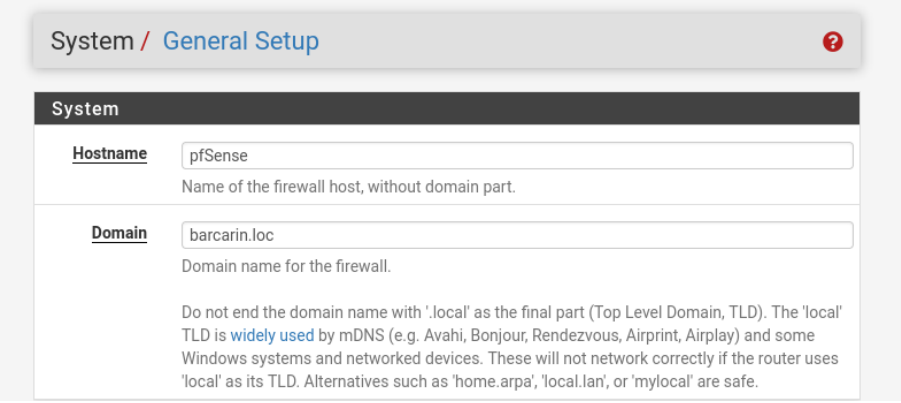
On ce reconnecte avec l'utilisateur qu'on viens de créé on retourne dans « User Manager » on clique sur le crayon de l'utilisateur « admin » :



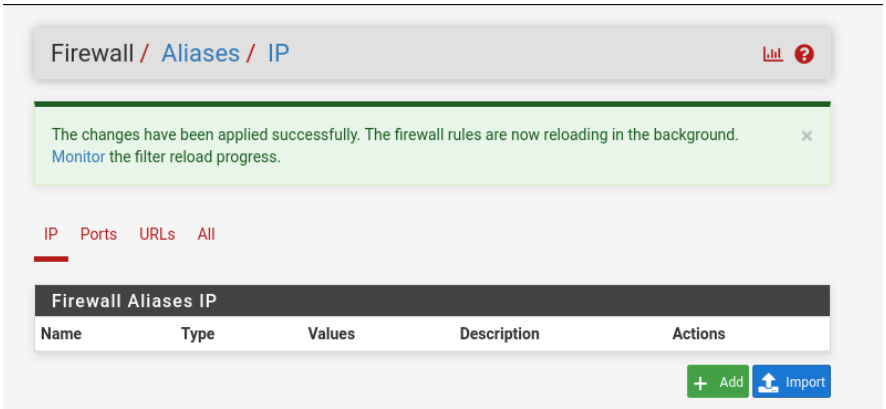
Puis on coche la case « This user connot login » :



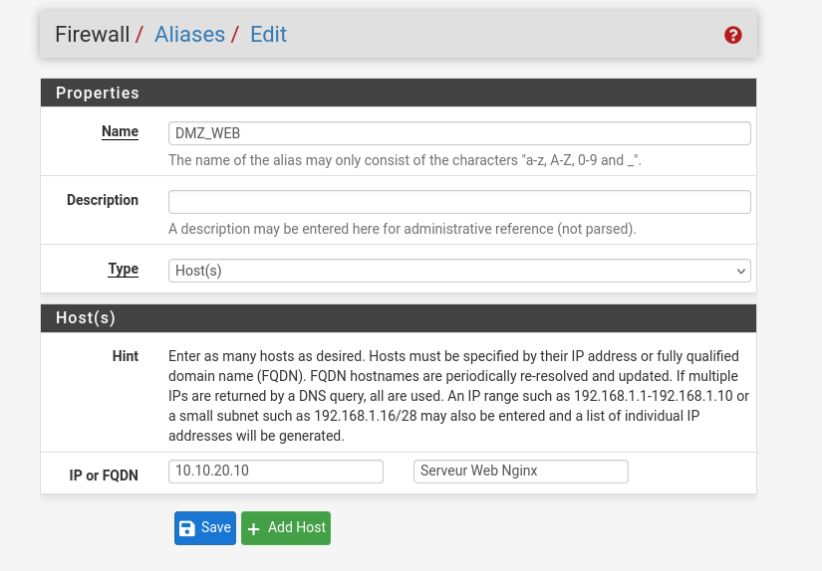
On peut ajouter notre nom de domaine également rdv dans System > Genral Setup et changer le domaine par le nôtre puis Save:



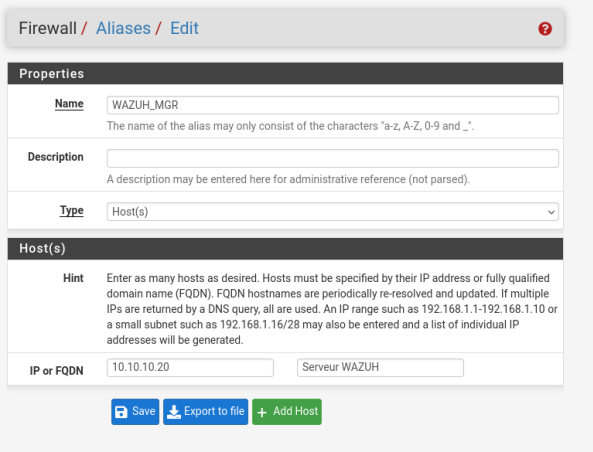
Voilà La configuration de base et Terminer on va passer maintenant Règle et sécurité à mettre en place : pour faciliter la mis en place des Règles on vas créer des Aliases pour ce faire rdv dans Firewall > Aliases :



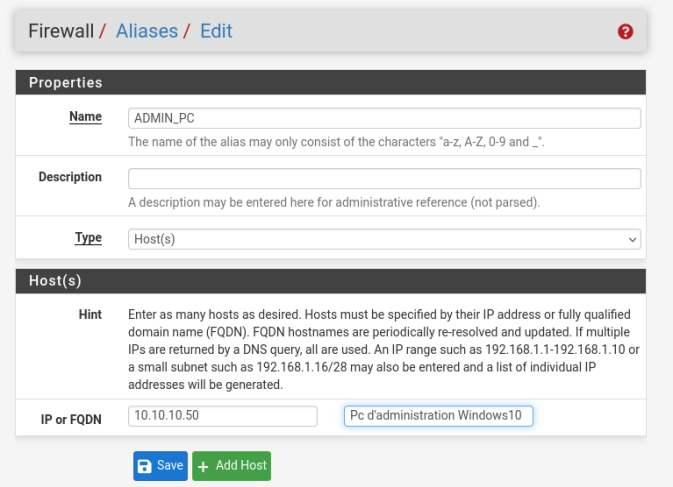
Cliquer sur Add : ce premier Aliase vas servir pour notre Serveur Web nginx qui ce trouvera dans notre DMZ : on ajoute un nom l'adresse IP est une courte descriptions on clique sur « Save » puis « Apply Changes »:



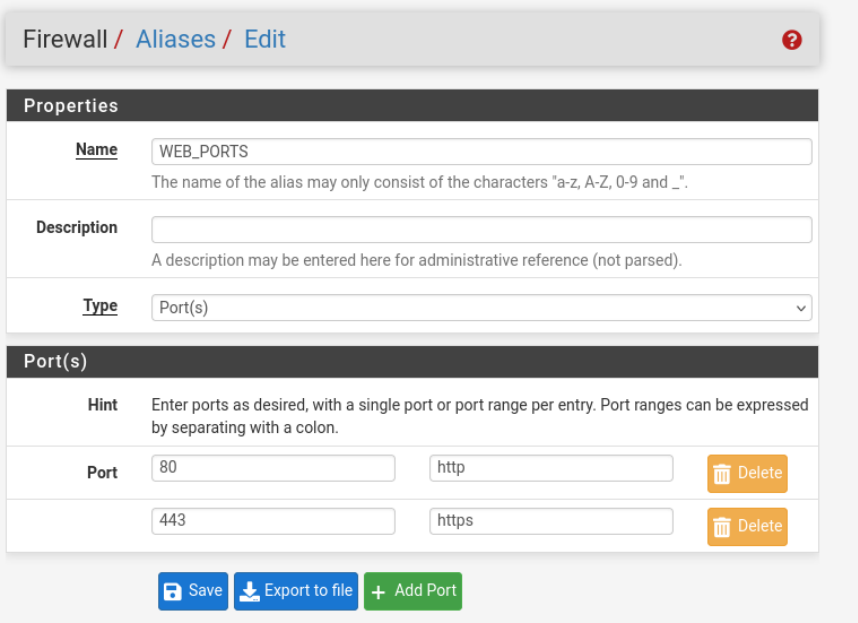
On fait de même pour notre Serveur Wazuh :



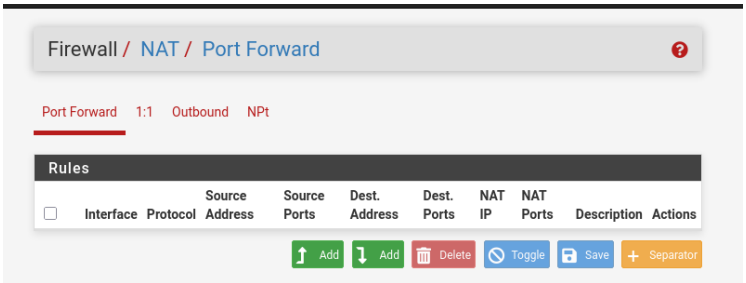
Est notre PC d'administration qui sera le pc Windows 10.



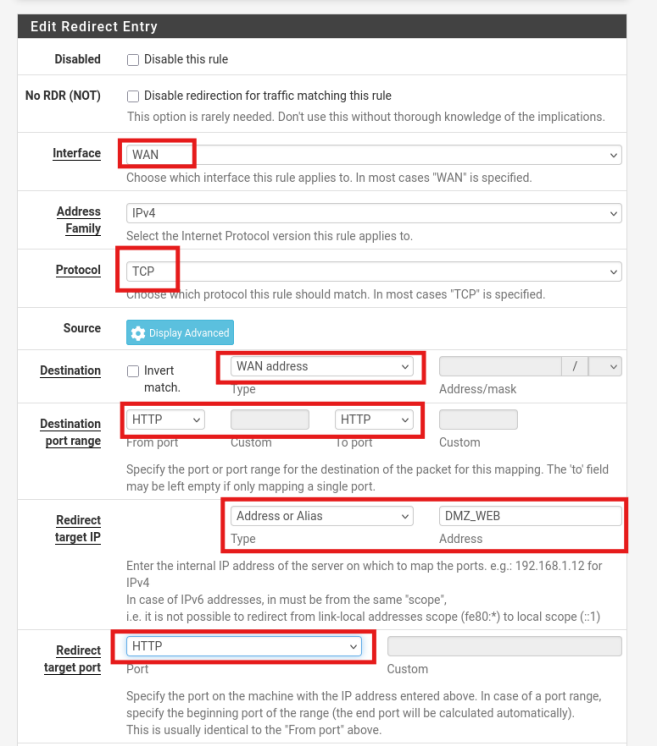
On vas aussi crée un alias pour le port 443 et 80 :



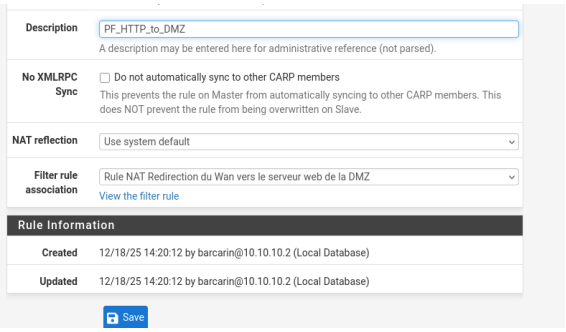
On passe maintenant au Règles de NAT rdv dans Firewall > NAT et dans l'onglet port Forward cliquer sur Add:



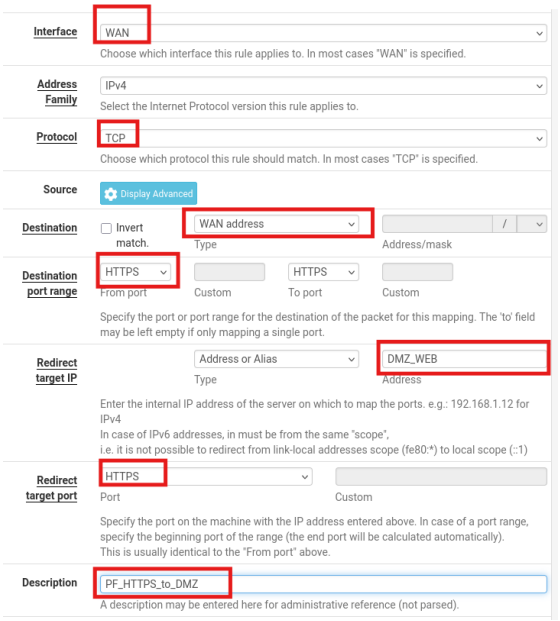
La première règle consiste à exposer notre serveur web sur internet et rediriger toute les requête faites sur notre interface WAN(Internet) sur le port 80 vers notre serveur web sur le port 80 qui se trouve dans notre DMZ.



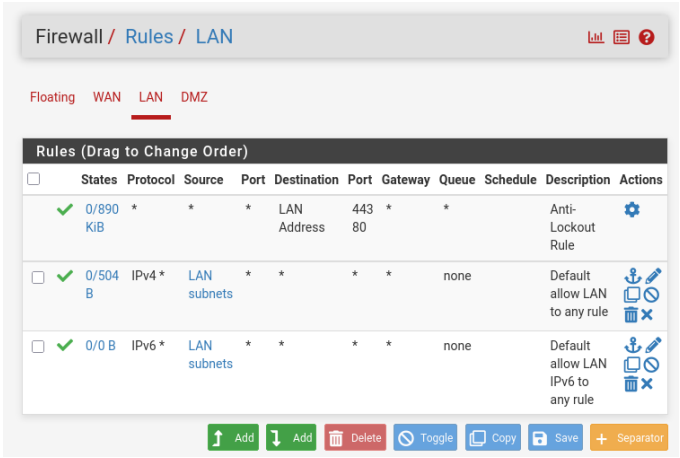
Une courte description et Save :



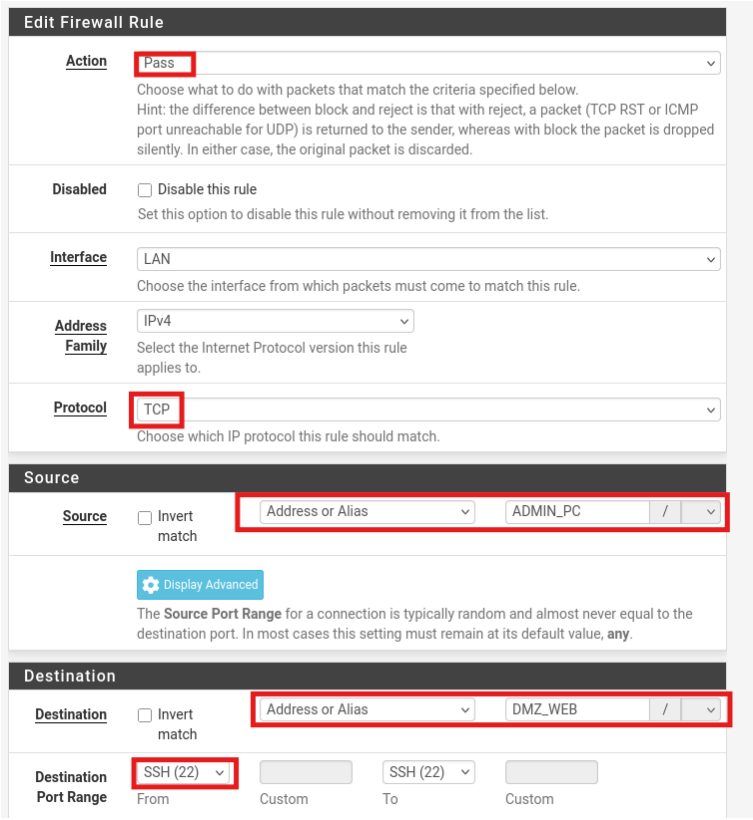
Faite la même chose mais pour HTTPS et le ports 443 « Save » et « Aply » :



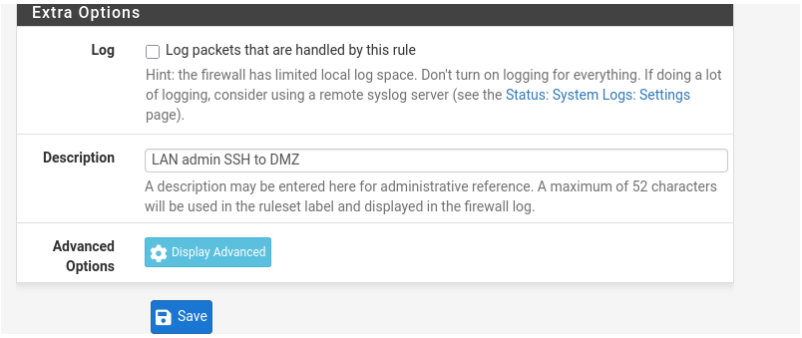
On n’a fini avec les règles du NAT on passe aux règles du LAN rdv dans Firewall > Rules > LAN :



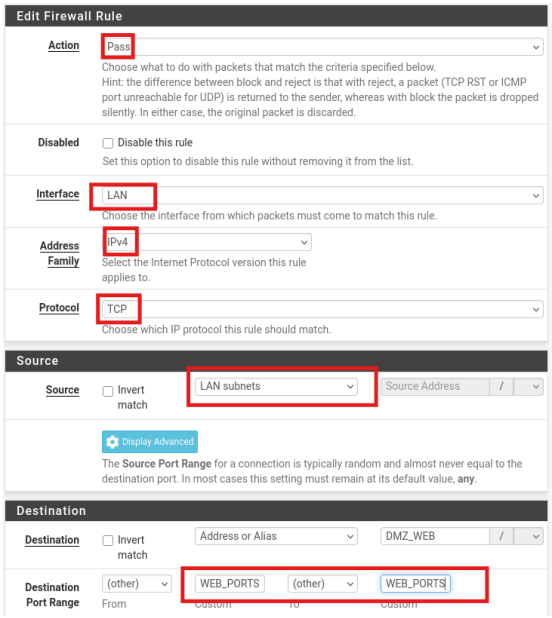
Cliquer sur Add flèche du Haut : on va créer une règle qui autorise seulement le PC admin a accéder via un tunnel SSH au Serveur Web Nginx dans notre DMZ.



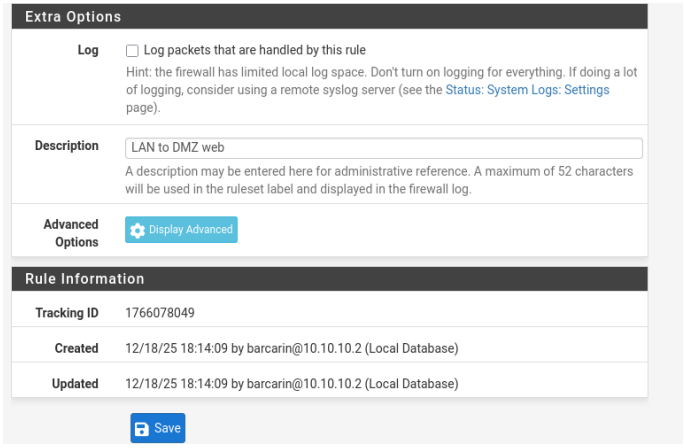
Une courte description et Save puis Apply :



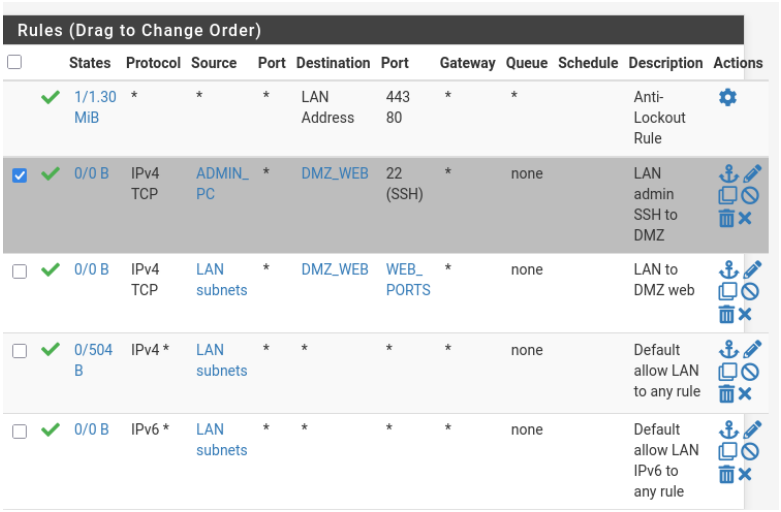
Prochaine Règle on autorise les paquet http et https a accédé à la DMZ depuis le LAN : Cliquer sur Add n'importe lequel (on réorganisera les règle après les avoir toute ajoutés) on commence par http :



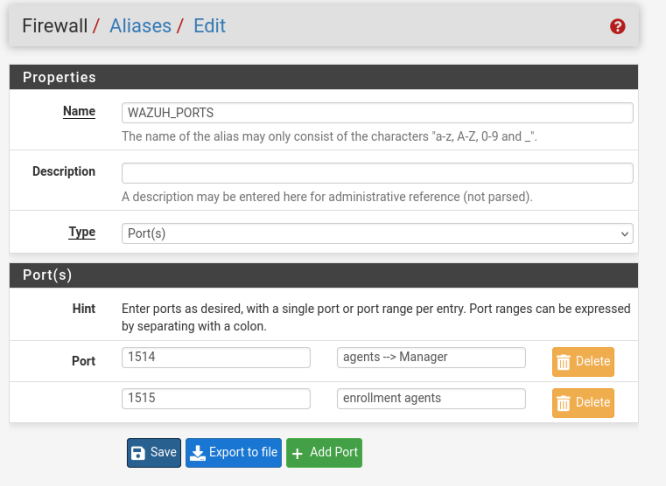
Courte description et Save puis Apply :



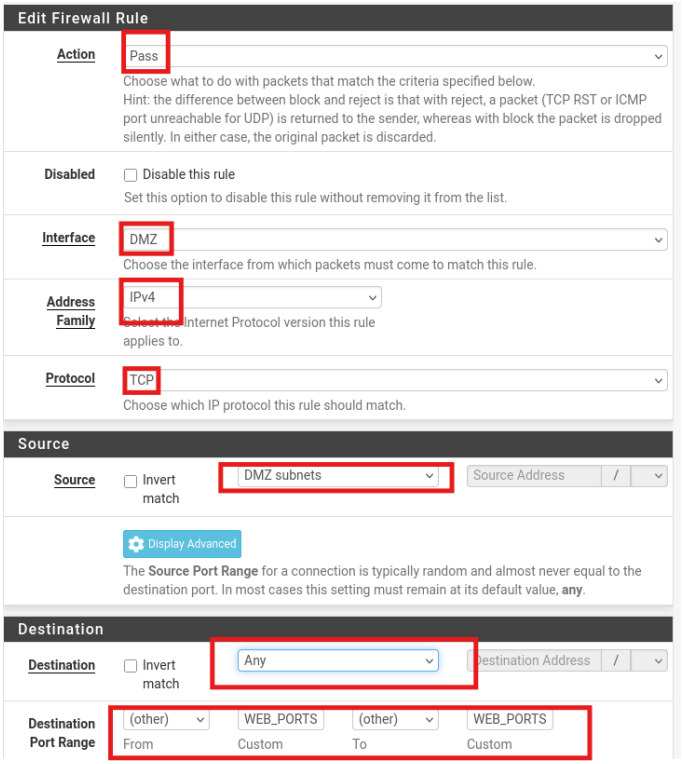
Pour l'ordre des règles m'était les comme si dessous :



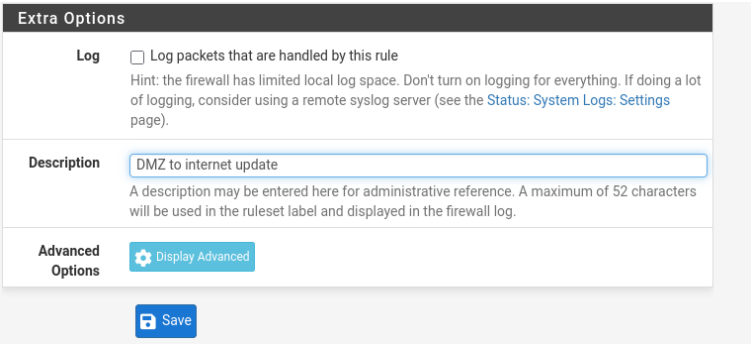
On passe maintenant à la DMZ (le plus important) : chaque règle on appuis sur Add flèche du haut : mais avant on vas cree un alias pour les port 1514 et 1515 pour notre serveur Wazuh :



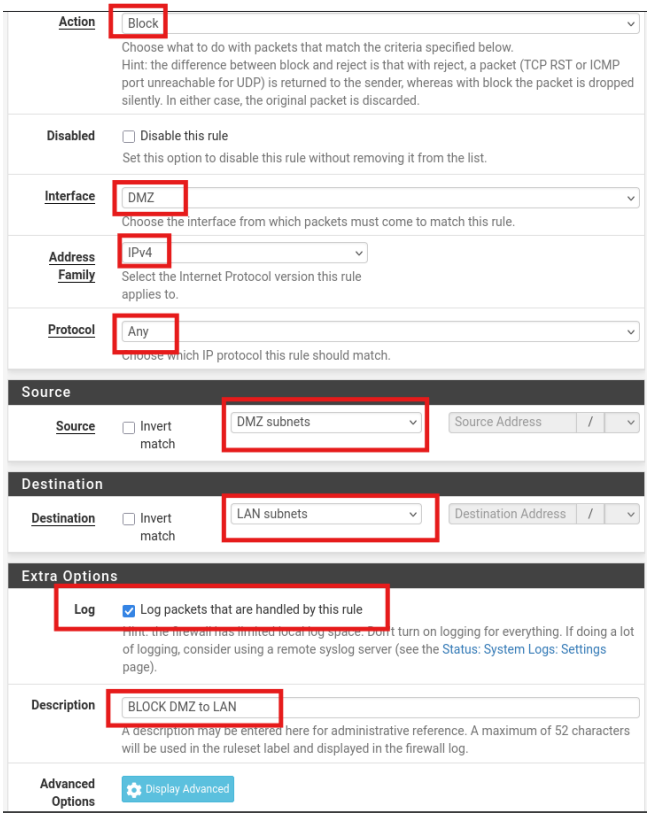
1er règle qui vas autoriser seulement http et https a sortir de la DMZ pour des MAJ notamment :



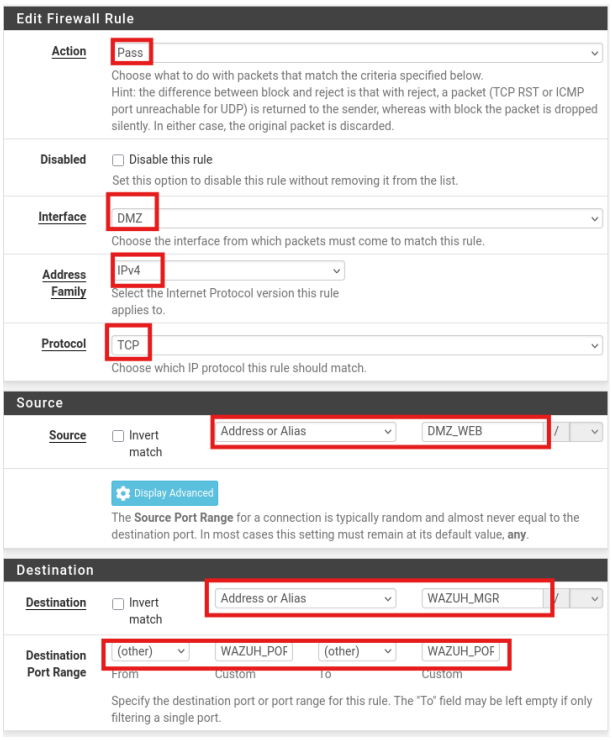
Courte description Save et Apply :



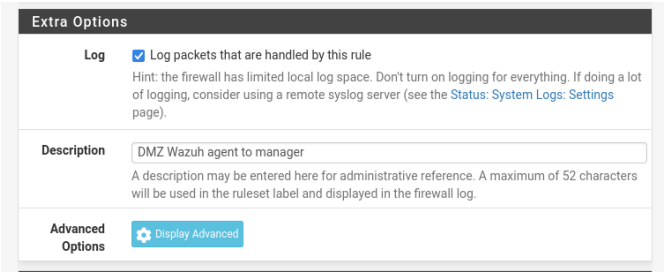
2éme règle on bloque tout ce qui vas de la DMZ vers le LAN pour cette règle il faut cocher « Log » (Preuve obligatoire) :



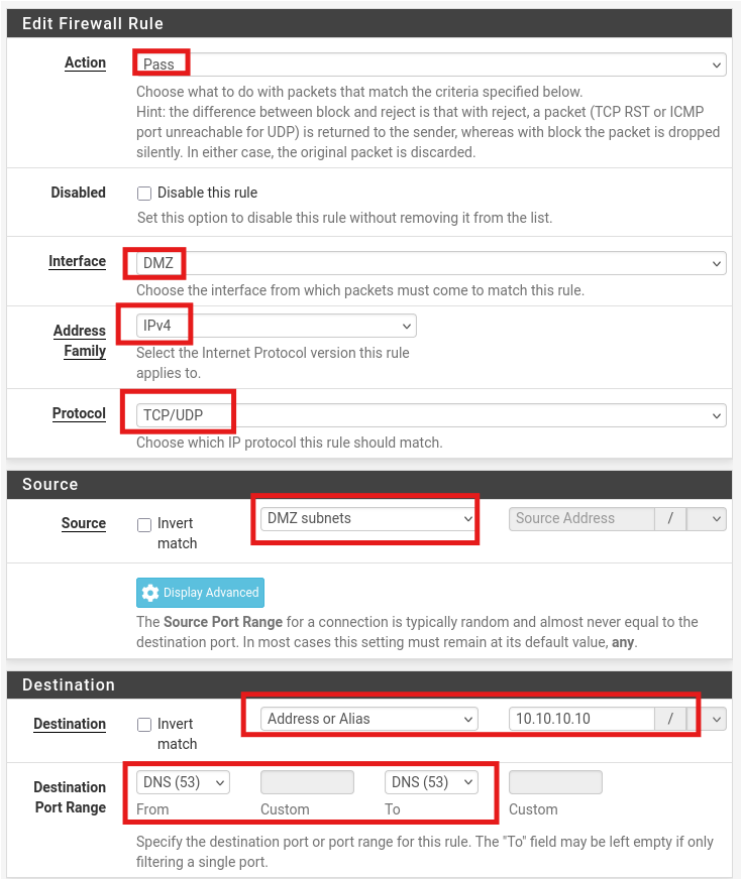
3eme règle on autorise les agent Wazuh et Wazuh Manager depuis la DMZ vers le LAN :



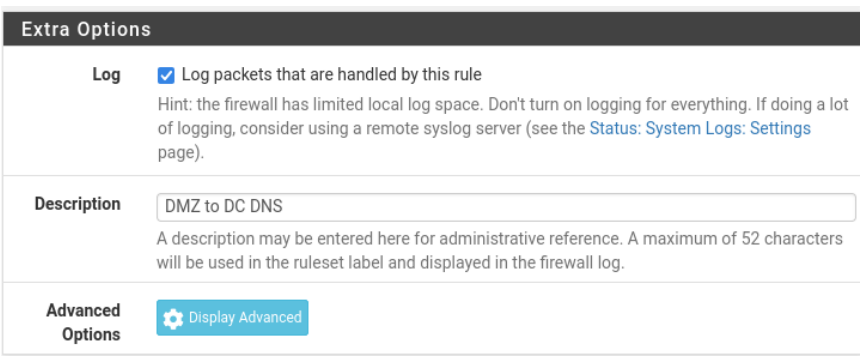
Courte description + Logs :



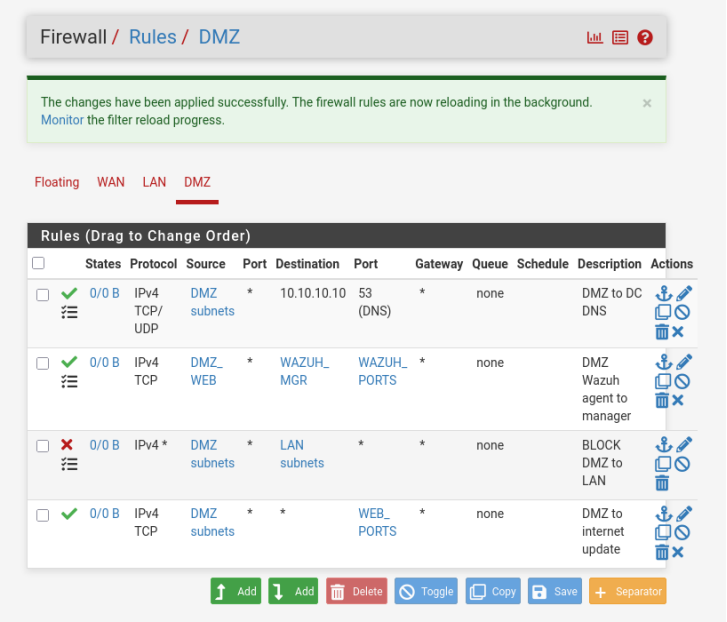
Dernier on autorise le DNS de notre windows serveur à faire de la résolution d'adresse de la DMZ vers le DNS :



Courtes descriptions + Logs :



Vos règles de Firewall dans la DMZ doivent exactement ressembler a ça :



La configuration de Pfsense et Maintenant terminer.