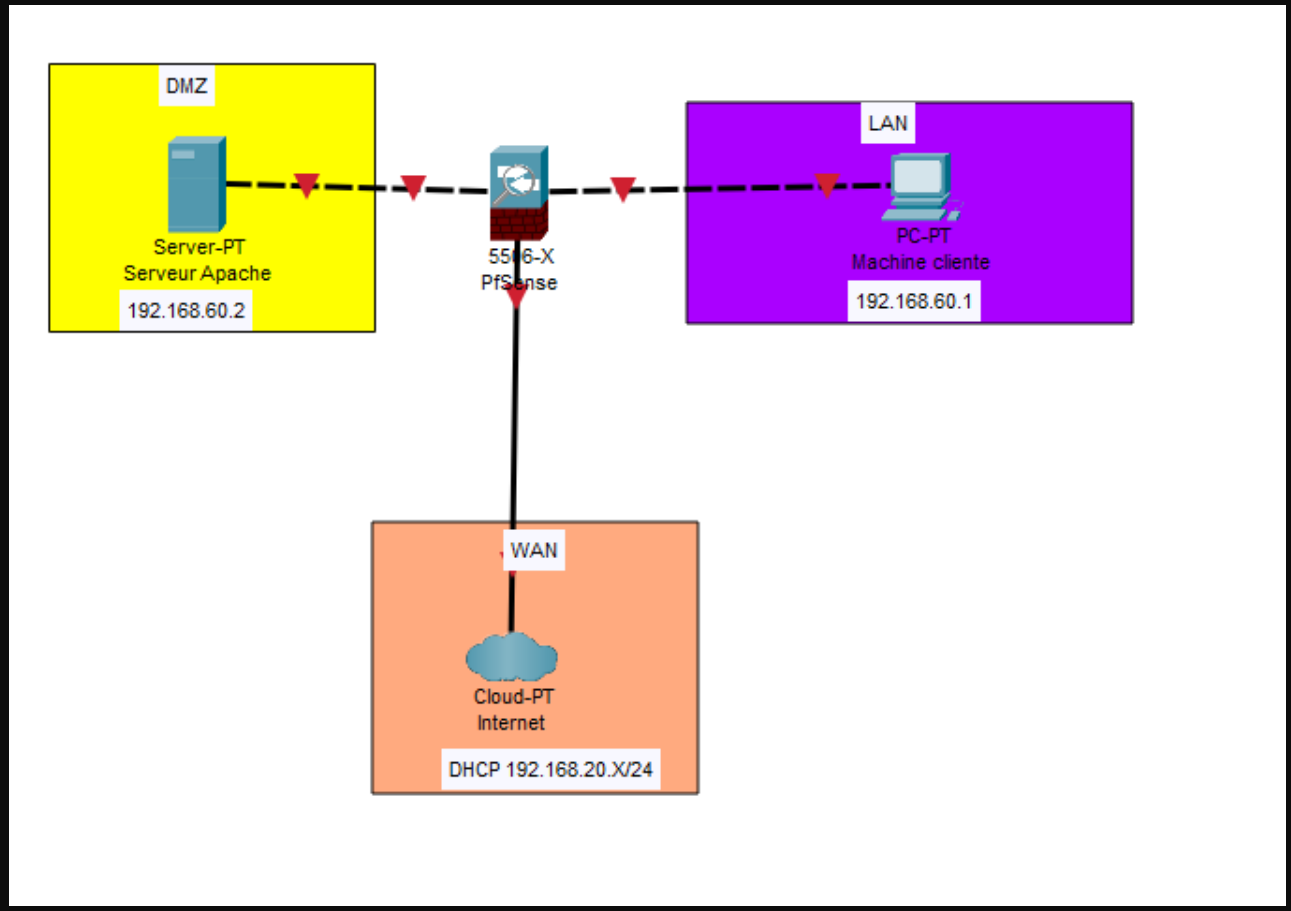
TP PfSense / DMZ

Contexte

La société Viktor souhaite mettre en place un serveur web accessible depuis son réseau interne LAN et depuis internet. Le choix de Pfsense a été fait pour répondre a ces attentes.

Dans le contexte du TP, internet debute dans le réseau de la salle de TP, en 192.168.20.X/24

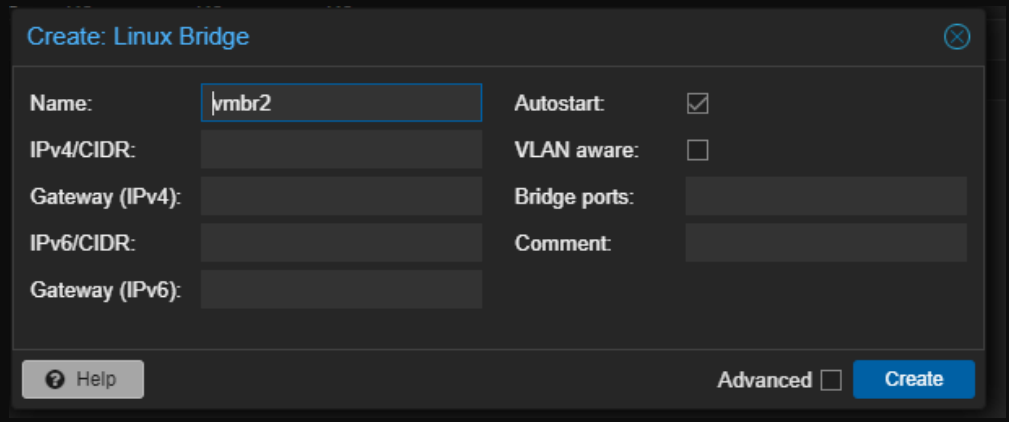
Nous avons l'infrastructure réseau suivante :



Création des cartes réseaux WAN, LAN et DMZ

Dans un premier temps, il faudra créer 2 cartes réseaux en plus de celle déjà existante pour le LAN et la DMZ, sur proxmox, il faudra se rendre dans network puis create, et Linux Bridge, ensuite nous pourrons renomer la carte comme nous le souhaitons, ici le nom est vmbr2. Ensuite il faudra ajouter la carte réseau à la machine virtuelle.

Pour installer une carte réseau, il faudra se rendre dans les paramètres hardware de la machine, puis cliquer sur add, network device et ajouter la carte réseau correspondant a celle crée précedemment



Network Device (net0)	virtio=BC:24:11:45:E4:48,bridge=vmbr0,firewall=1
Network Device (net1)	virtio=BC:24:11:C5:96:4F,bridge=vmbr1,firewall=1
Network Device (net2)	virtio=BC:24:11:5F:88:72,bridge=vmbr2,firewall=1

Cartes réseau de la machine pfsense

Network Device (net0)	virtio=BC:24:11:F7:10:83,bridge=vmbr1,firewall=1

Cartes réseau de la machine sur le LAN W10

Network Device (net0)	virtio=BC:24:11:B8:C5:9D,bridge=vmbr2,firewall=1

Cartes réseau de la machine LAMP dans la DMZ

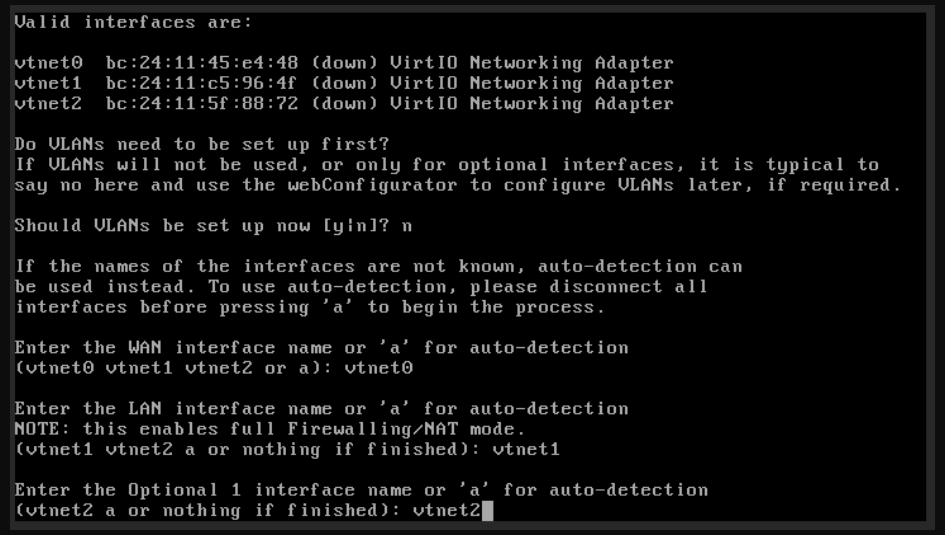
Installation Pfsense

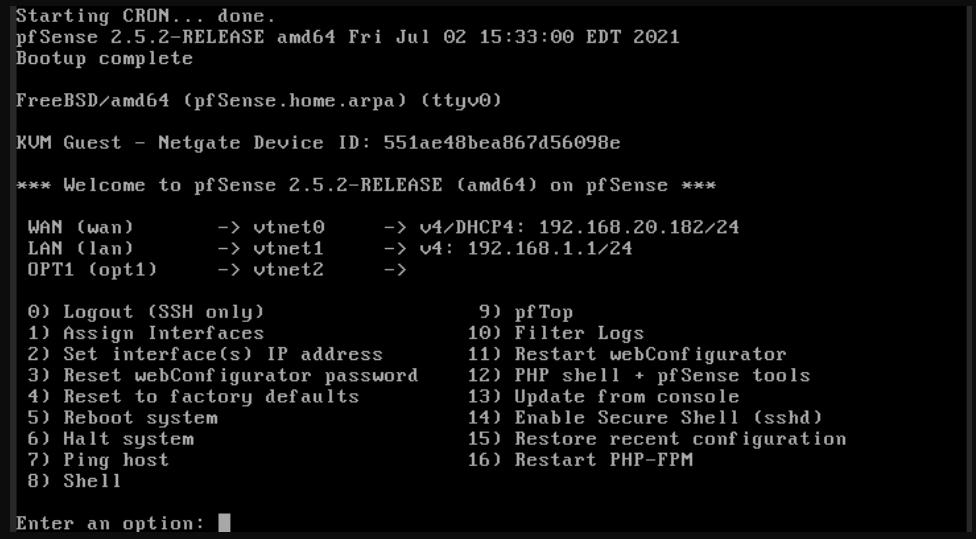
Au niveau de l'installation de pfsense, il suffit de choisir la configuration du clavier et de choisir le disque ou sera installé l'os, pour le reste nous pouvons appuyer sur suivant jusqu'a la fin de l'installation.

Configuration Pfsense

Dans un premier temps, il faudra installer PfSense. Ensuite, lors de la configuration de la machine, il faudra renseigner les informations pour l'interface WAN (vtnet0) , pour l'interface LAN (vtnet1) et pour l'interface Optional 1, qui sera notre interface DMZ (vtnet2).

Ensuite il faudra selectionner l'option 1 pour paramétrer les interfaces.





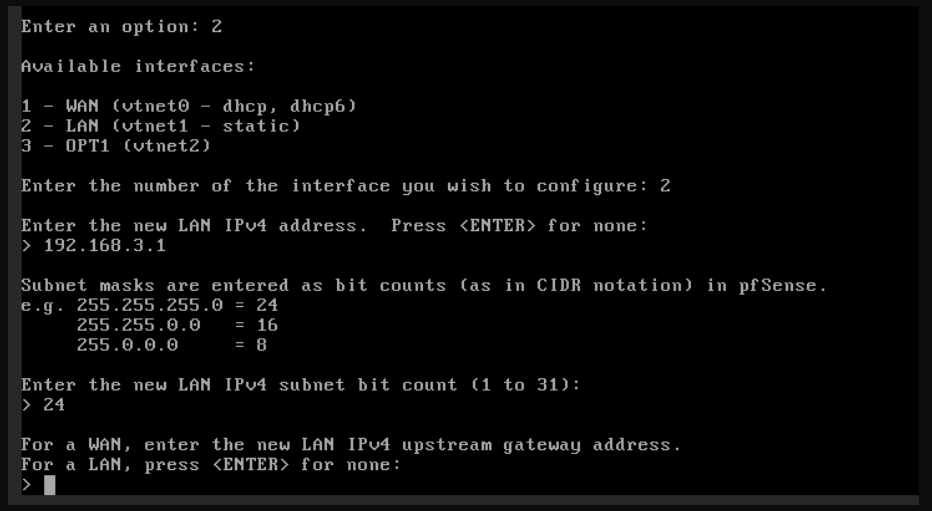
Paramétrage du LAN

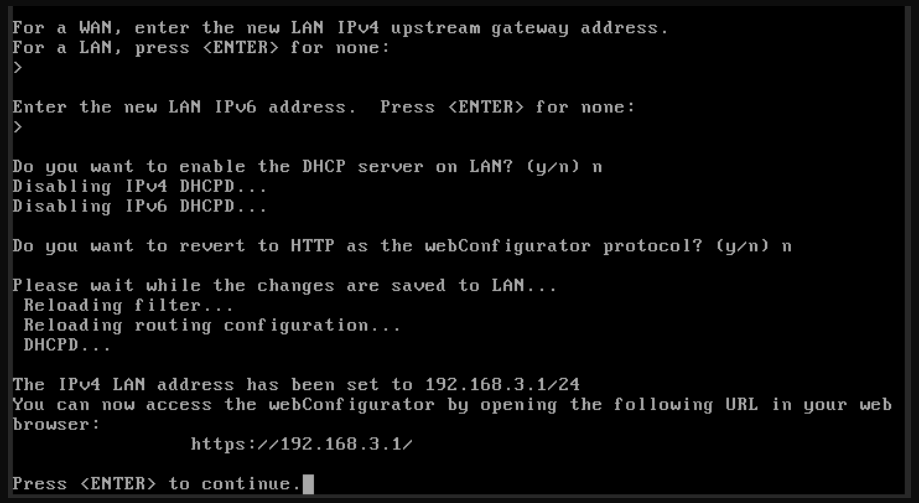
De base, l'IP du LAN est 192.168.1.1 mais nous pouvons la changer.

Dans un premier temps, je selectionne l'interface LAN qui est l'option 2, ensuite je rentre une adresse IP qui sera 192.168.3.1

Ensuite je paramètre le masque qui sera 255.255.255.0 donc 24.

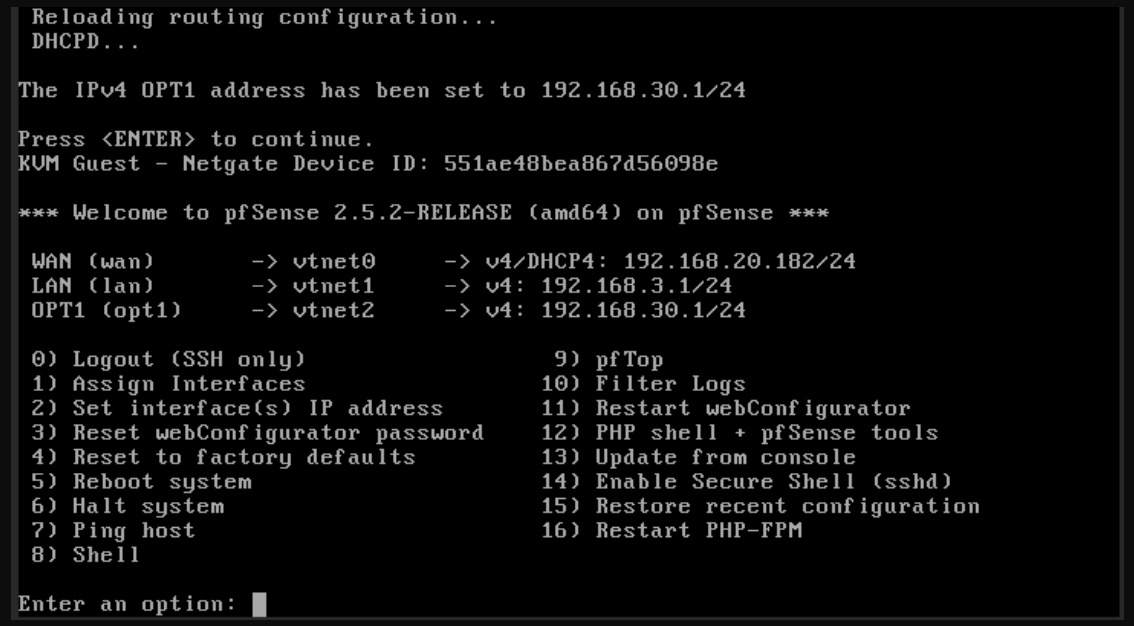
Ensuite nous pouvons passer tous les paramètres proposés.





Paramétrage de la DMZ

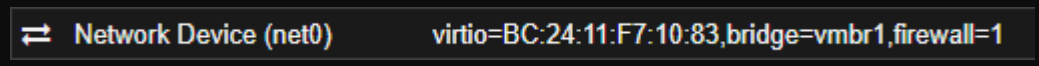
Pour ce qui est de la DMZ, la configuration est la même, pour ma part j'ai fixé l'IP 192.168.30.1 avec un masque en 24

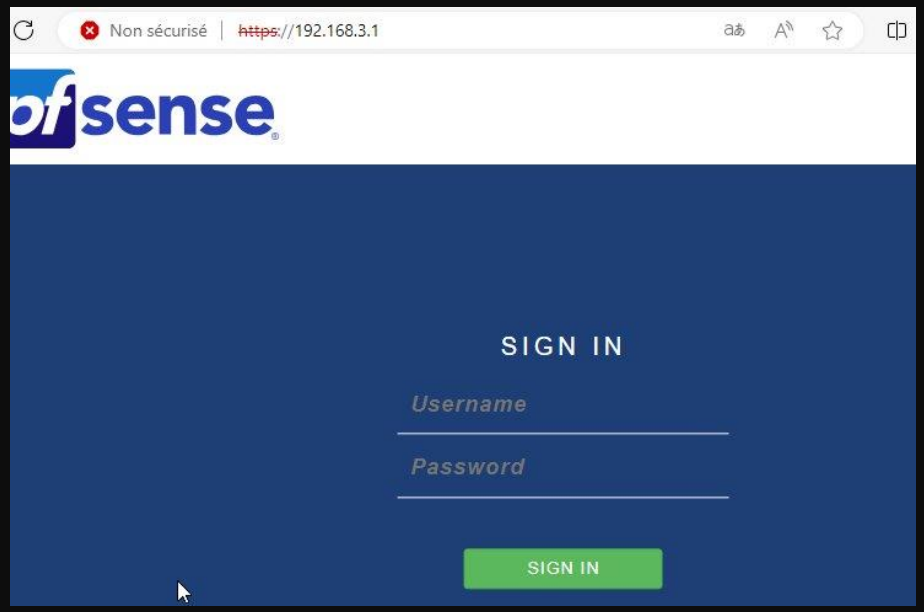


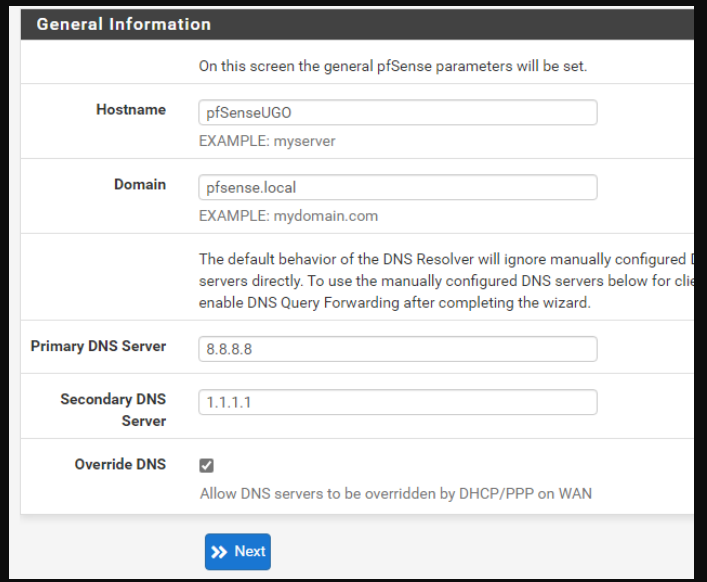
Connexion a l'interface pfsense

Pour pouvoir accéder au panneau de configuration du pfsense, il faudra que la carte réseau soit la même que celle que le lan tout a l'heure, donc vtnet1. Ensuite nous pourrons accéder a l'interface du pfsense via l'ip que nous avons fixé précédemment, donc 192.168.3.1.

Une fois sur cette page, nous pourrons configure le pfsense, pour ma part j'ai modifié le nom d'hôte, le DNS primaire pour 8.8.8.8 qui est le DNS google et le second serveur dns pour 1.1.1.1







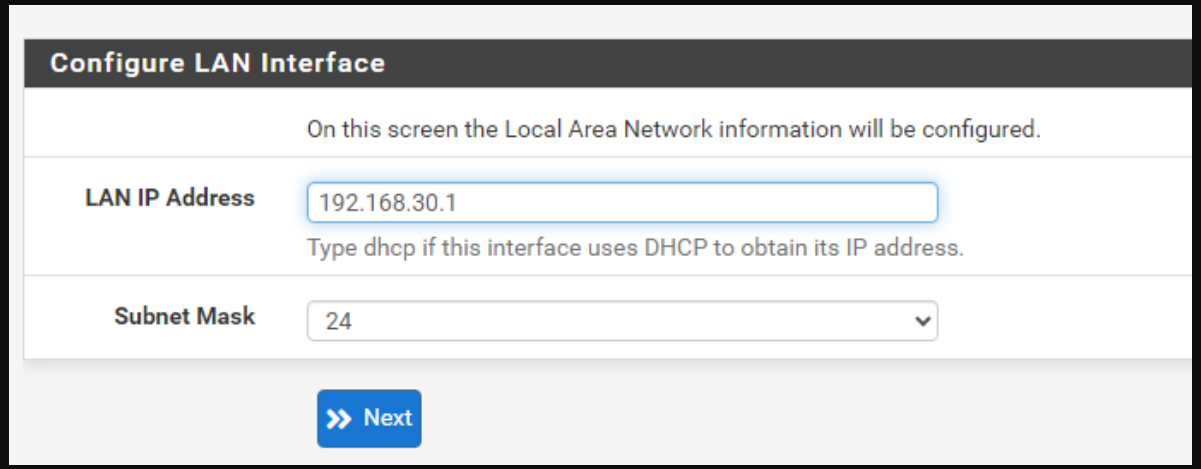
Configuration Pfsense

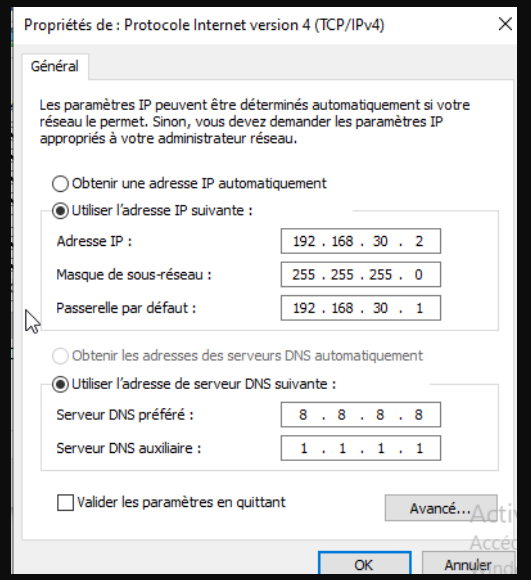
Ensuite, à l'étape suivante vous pourrez choisir le serveur de temps, pour ma part j'ai choisi celui de paris.
Pour la configuration de l'interface WAN, il n'y a rien a modifier.

Pour celle du LAN, nous pouvons modifier l'adresse de l'interface LAN pour correspondre à l'adressage défini précédemment, j'ai donc rentré l'IP 192.168.30.1 avec le masque 24. Par consequent, je change l'adresse IP de ma machine Windows pour qu'elle reste sur le réseau LAN.

Ensuite il faudra modifier le mot de passe admin.

Et la configuration est terminée, vous pouvez faire suivant jusqu'au reload et a la fin de la configuration



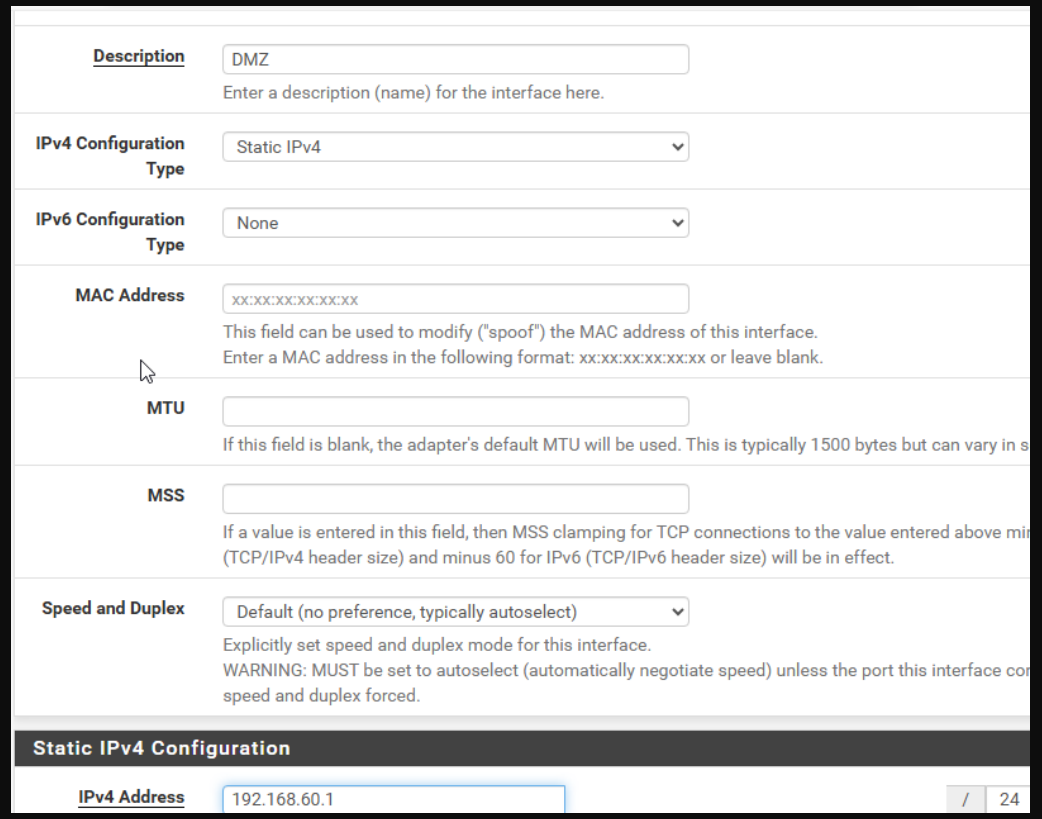


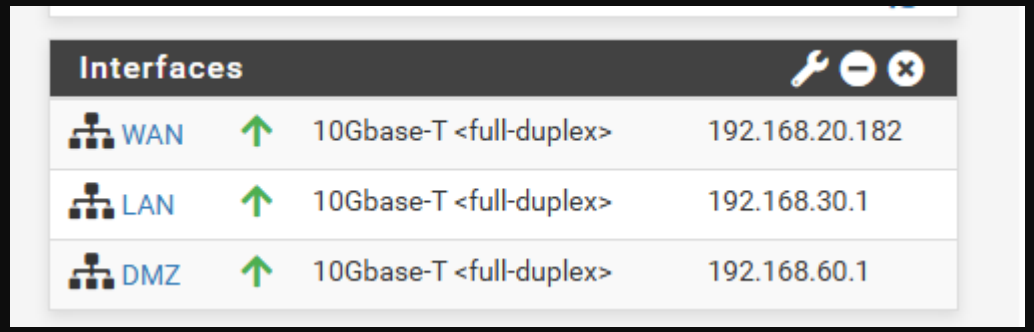
Création DMZ

Pour assimiler l'interface restante pour la carte vtnet2, il faudra se rendre dans interface, et assignments et cliquer sur add a coté du network port vtnet2.

Ensuite il faudra cliquer dessus, et cocher la case enable afin de l'activer. Je lui donne un nom dans Description qui sera DMZ. L'IP sera une IP statique et l'IP sera 192.168.60.1 avec un masque en 24.

Ensuite nous pourrons sauvegarder et appliquer la configuration.



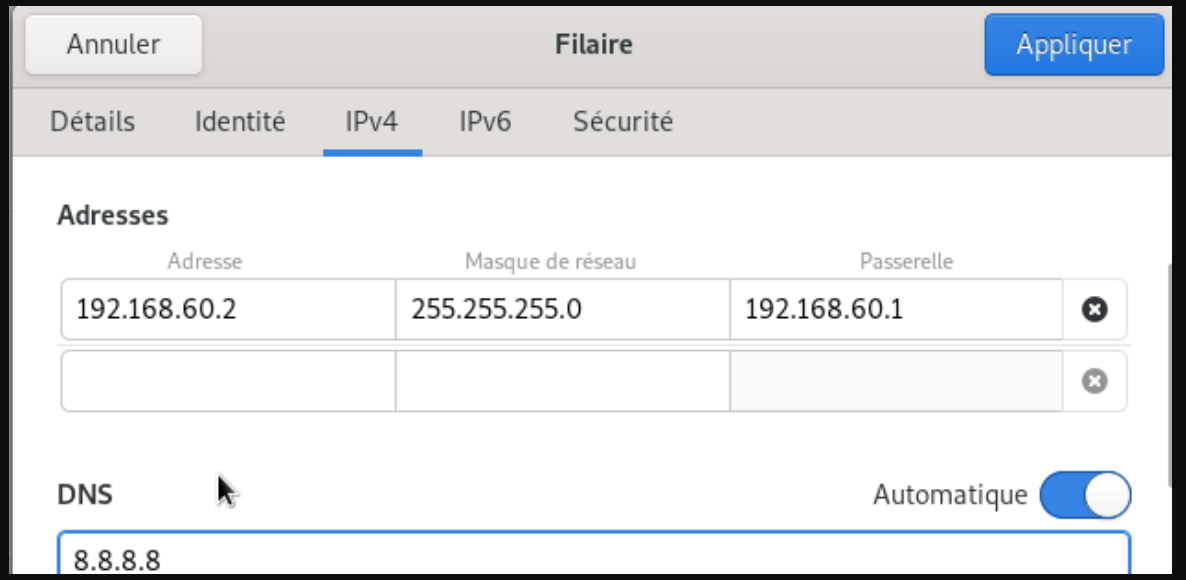


Nous pouvons constater que nous avons nos 3 interfaces actives

Mise en place du serveur Apache

Pour mettre en place le serveur apache, nous aurons besoin d'une nouvelle machine virtuelle avec la carte réseau de la DMZ et qui se situera sur le même réseau, de ce fait, je fixe mon IP en 192.168.60.2/24 avec l'adresse de la DMZ en passerelle.

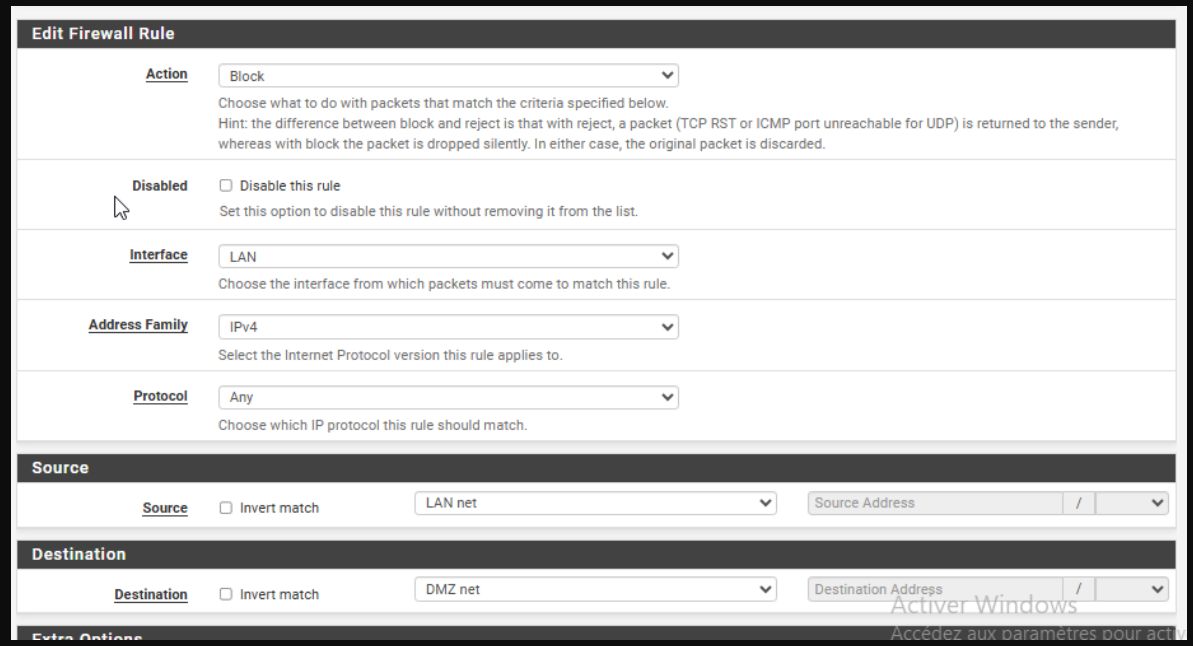
Ensuite nous pourrons installer apache avec la commande apt install apache2 et modifier le fichier html avec la commande nano /var/www/html/index.html

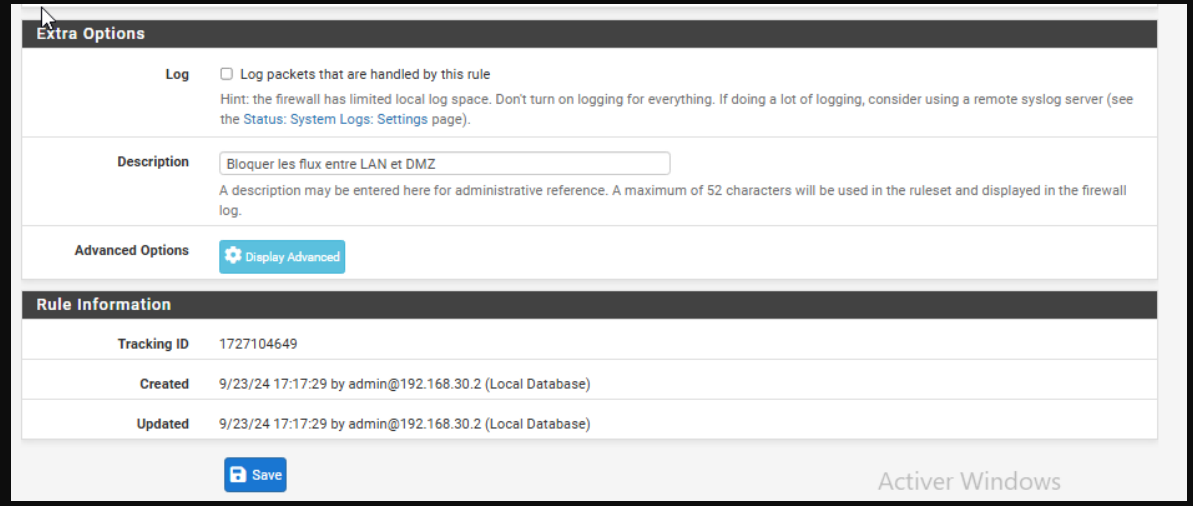


Mise en place de règles LAN

Entre le LAN et la DMZ, nous avons uniquement besoin que le port 80 soit accessible, donc il faut mettre en place des règles de pare-feu sur le LAN. Pour se faire, il faudra se rendre dans firewall, puis rules et dans LAN, ensuite il faudra cliquer sur le bouton Add avec la fleche vers le haut.

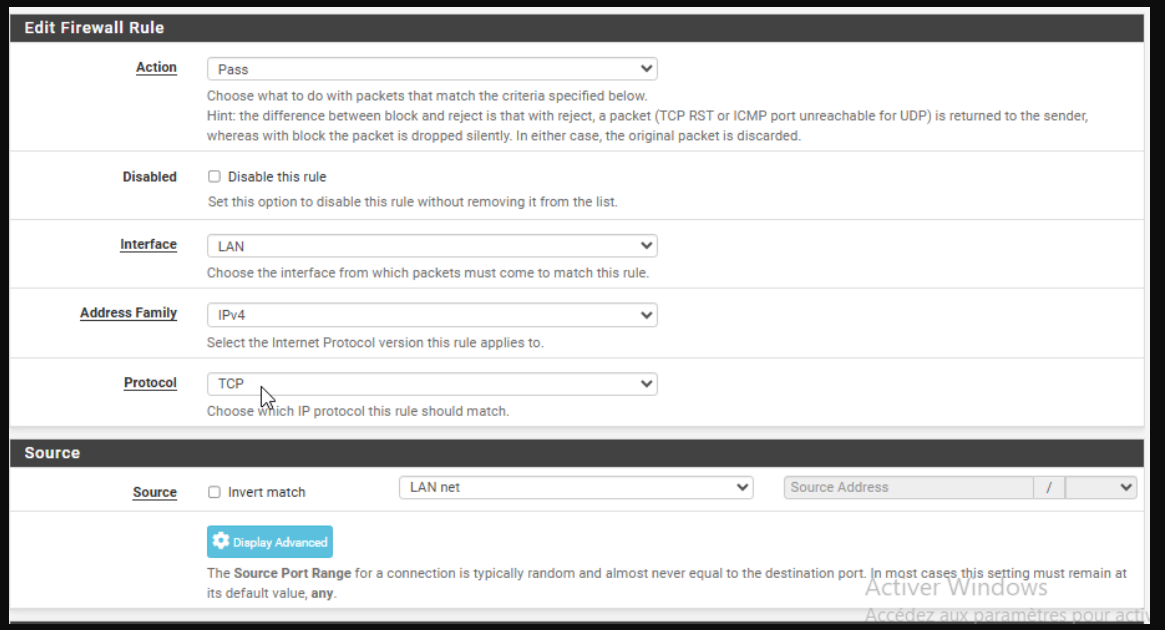
Dans action il faudra selectionner block, pour tous les protocols donc any. La source sera le LAN net et la destination le DMZ net.

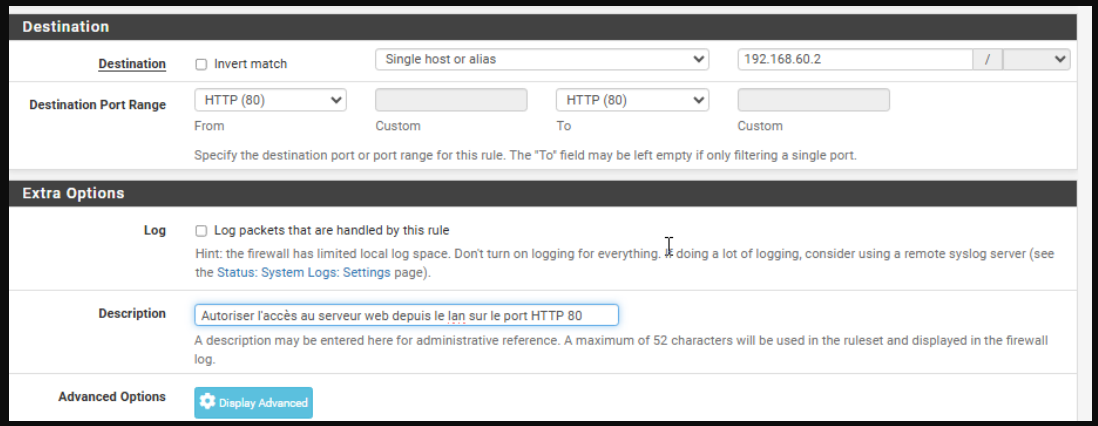




Mise en place de règles LAN

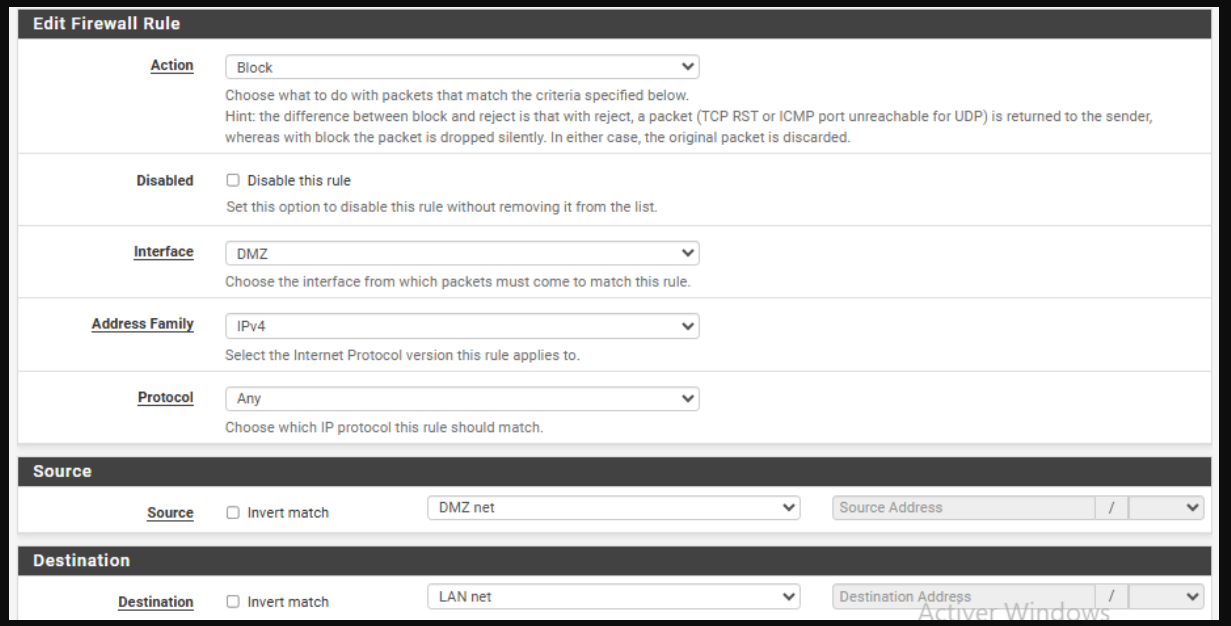
Pour pouvoir acceder au serveur Web sur le LAN sur le port 80, il faudra créer une règle particulière. Il faudra autoriser avec pass, les requetes qui ont pour source le réseau LAN en direction de l'hote 192.168.60.2 qui est l'IP de la DMZ pour le port 80 qui correspond au HTTP

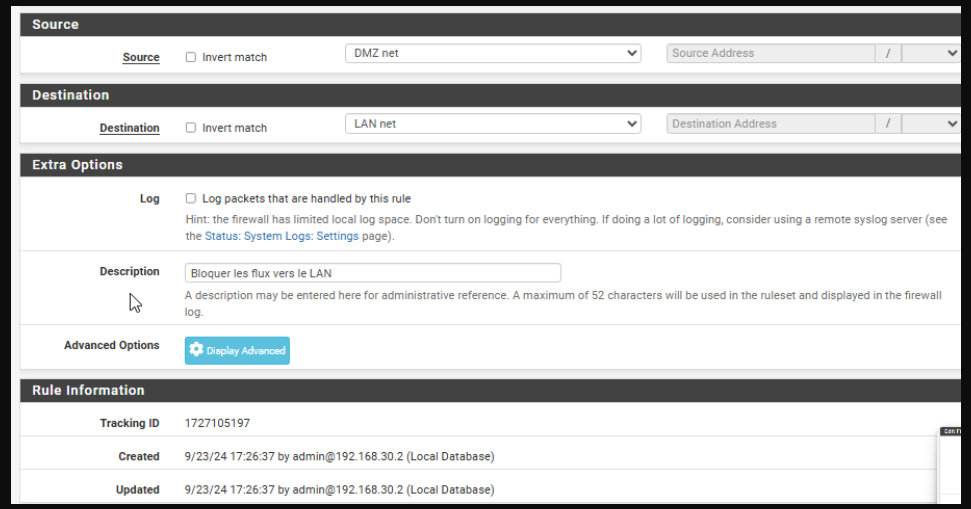




Configuration des règles DMZ

Sur l'interface DMZ, nous allons bloquer les flux en direction du LAN. Il faudra donc bloquer tous les protocoles sur l'interface DMZ avec comme source, le réseau DMZ et pour destination le réseau LAN.



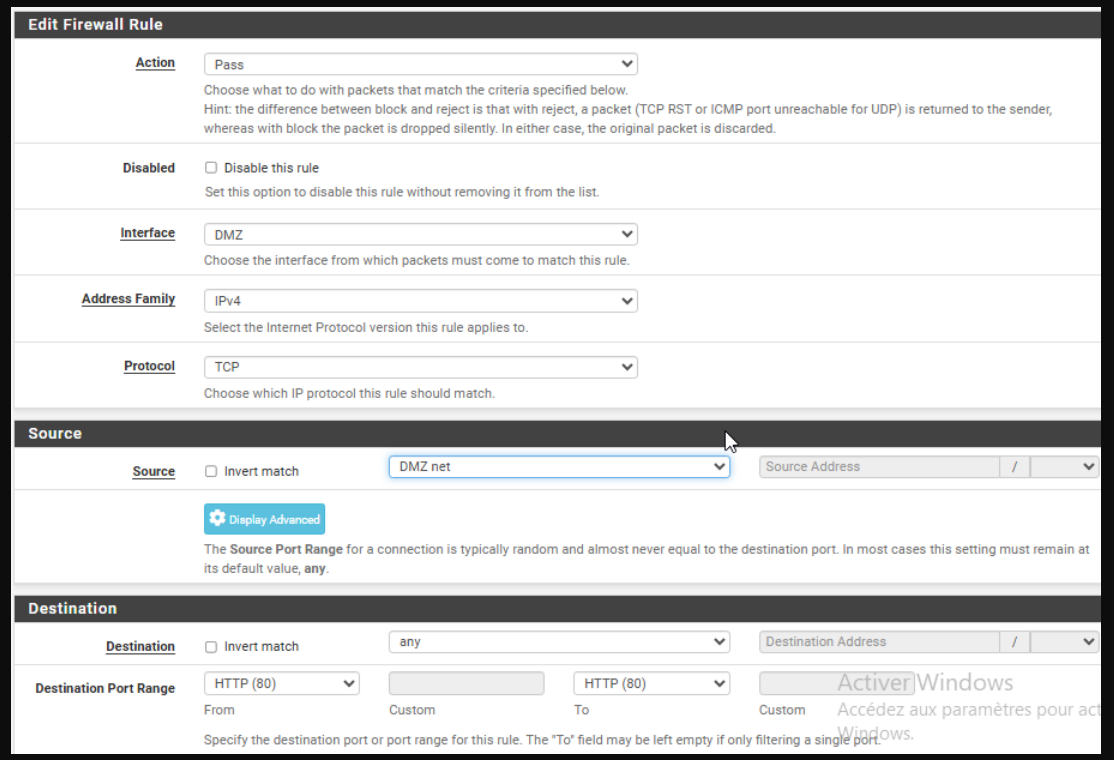


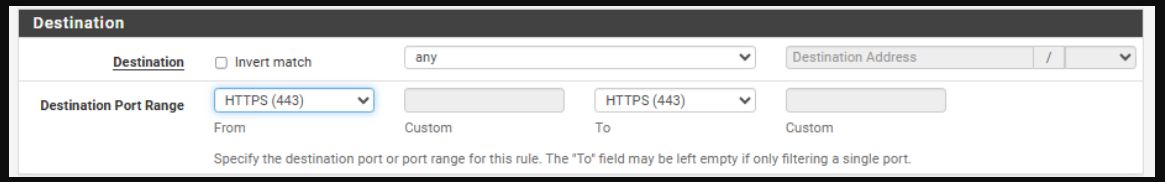
Configuration des règles DMZ

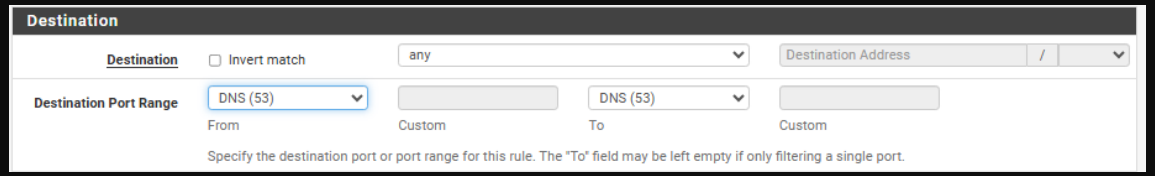
Ensuite nous allons créer une règle en dessous avec le bouton add avec la fleche vers le bas, pour autoriser la DMZ a acceder a internet par le port 80.

Il suffira de dupliquer la règle pour autoriser les protocoles DNS et HTTPS.

Ensuite nous pourrons sauvegarder



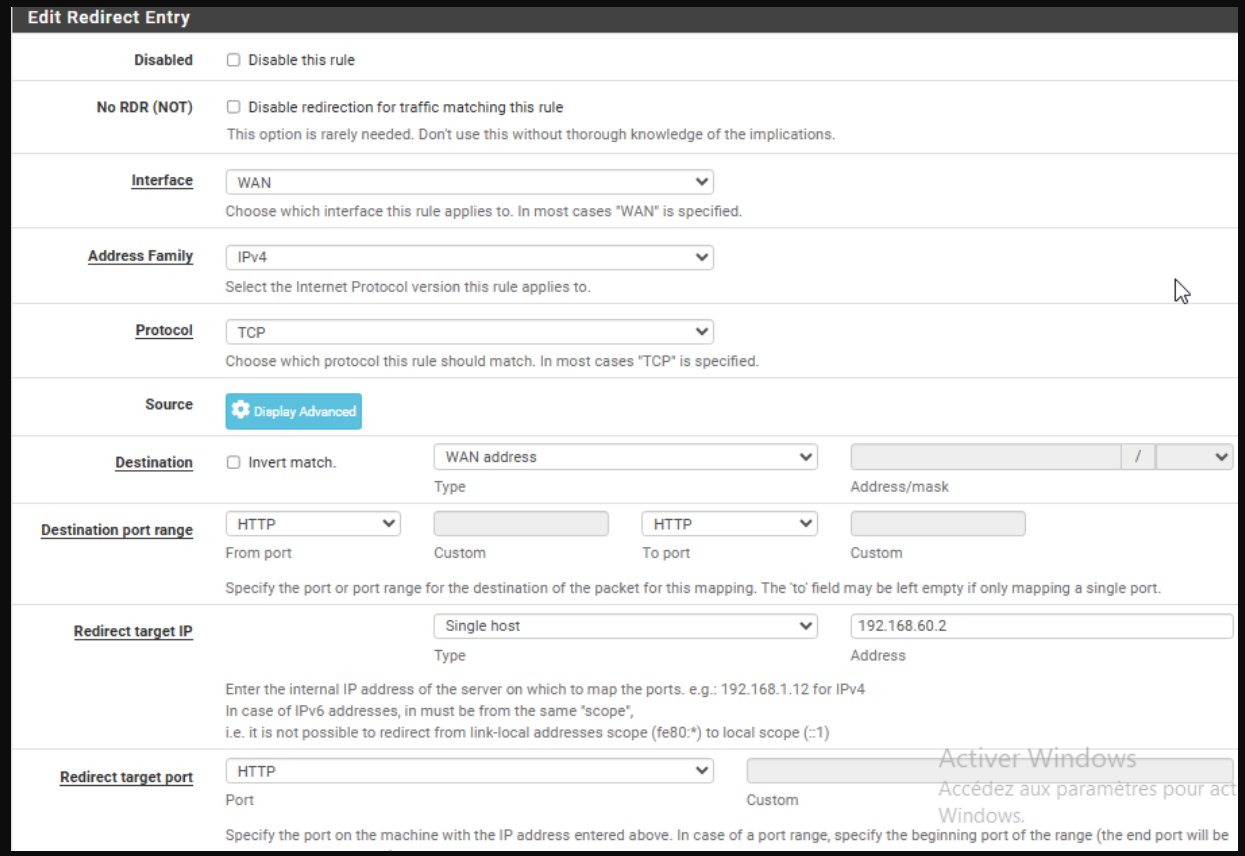


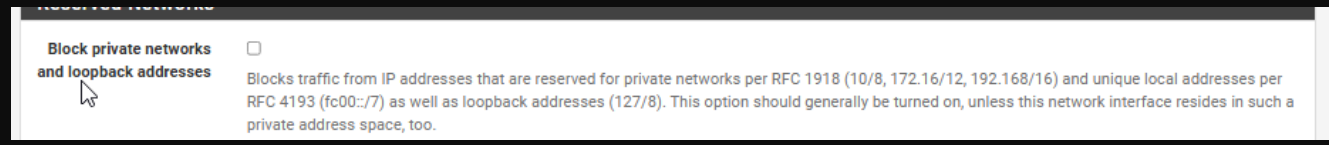


Création des règles NAT

Pour gèrer l'accès du site Web depuis le WAN, il faudra se rendre dans NAT, puis Port Forward pour créer une règle qui concernera les flux de l'interface WAN en TCP sur l'adresse du WAN et nous créerons une redirection des flux HTTP sur l'IP du Wan seront redirigés vers l'IP 192.168.60.2 qui est l'ip du serveur

Il faudra désactiver l'option Block private networks and loopback addresses sur l'interface WAN qui bloque les addresses du RFC 1918, et lorsque nous nous connectons depuis le WAN, notre adresse est en 192.168.20.X donc nous nous retrouvrions bloqués.





Tests

Nous pouvons constater que nous avons accès a la DMZ depuis le LAN (premier screen) et depuis le WAN (deuxieme screen)