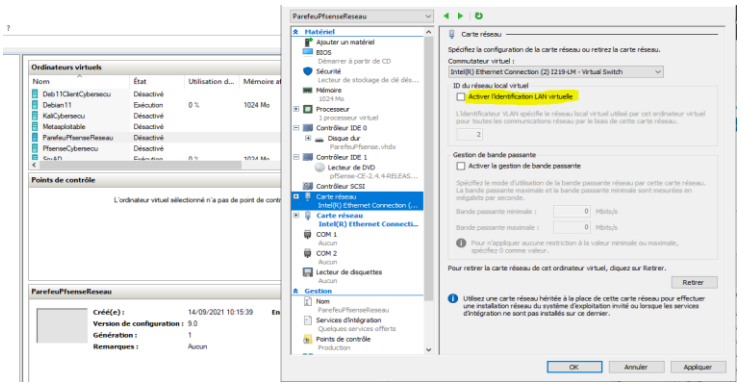
Installation pfSense

Il nous est demander de brancher notre machine virtuelle dans 2 vlans via un port tagué

Pour cela nous allons ajouter 2 commutateur externe qui seront relier à la carte réseau du PC et qui comporteront 2 étiquettes de 2 vlan différents (VLAN ID)

Une interface virtuelle comportant comme vlanID 60
Une deuxième interface virtuelle comportant comme vlanID 30

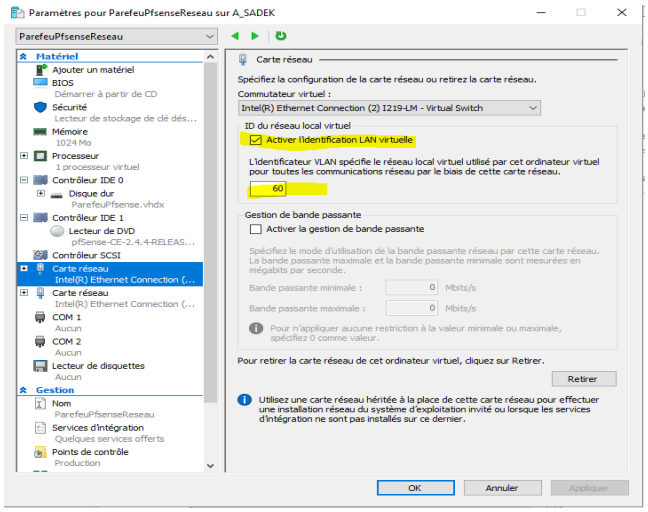
Et mes deux DMZ qui seront dans le vlan 40 mais dans un commutateur interne



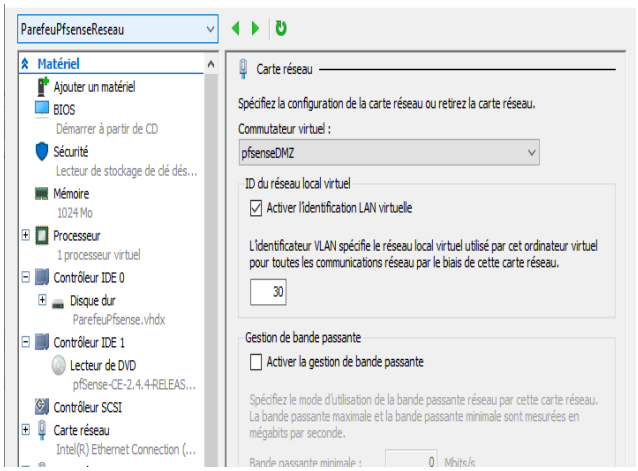
La première interface réseau est celle la

-Je vais la modifier je vais commencer par activer l'identification VLAN

Et spécifier le vlan 60



Et ici le commutateur interne

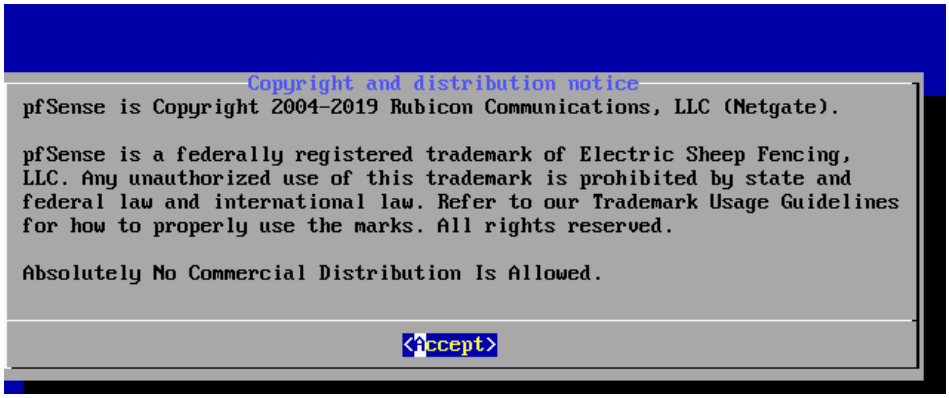


J’ai configuré les 3 interfaces comme ceci

Je lance la VM pfsense

L’écran d’installation s’affiche

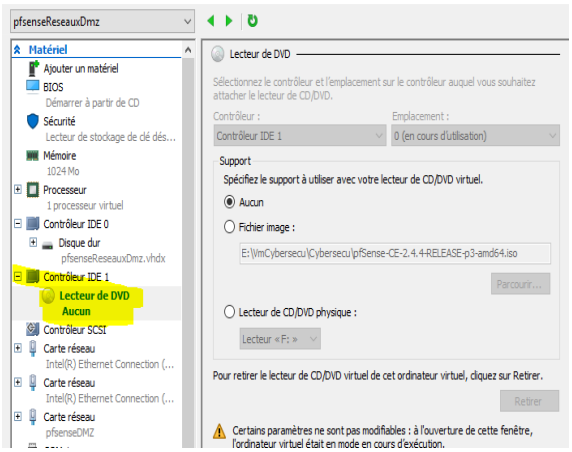
Je ne choisis rien je laisse sa ce lancera automatiquement



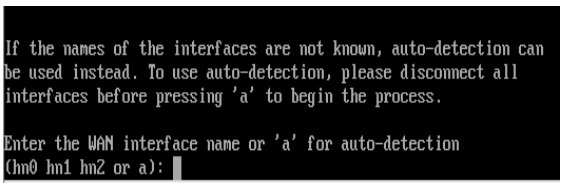
J’accepte

- Ensuite je sélectionne install pfsense
- Ensuite je choisis le clavier francais et je lance une installation automatique
- Une fois l’installation terminer on me demande si je veux ouvrir un shell
- Je repond non
- On me demande de redémarrer
- Je redémarre

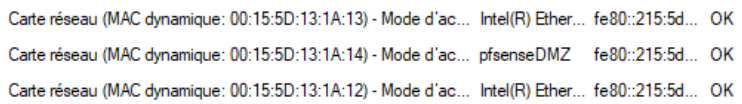
- Ensuite j'enlève le cd virtuel d'installation sinon il reboot sans cesse sur l'écran d'installation je vais dans les paramètres de la vm et je coche « Aucun »



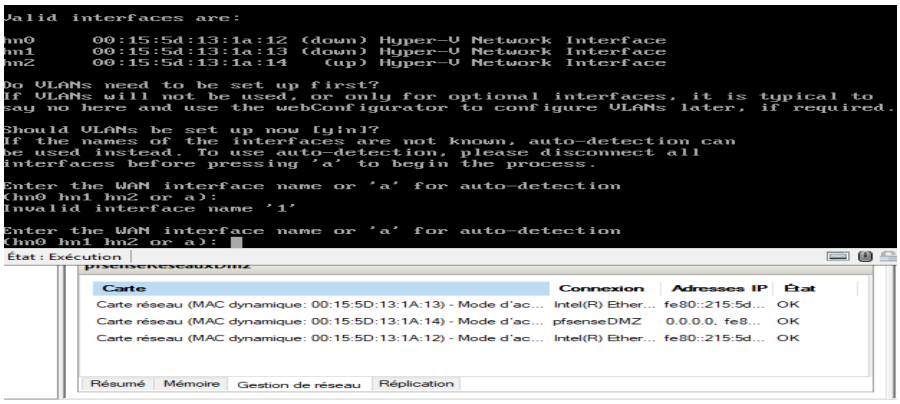
Je dois préciser quelle interface est quoi LAN ou WAN



Du coup je suis partit dans les détails réseau de la VLAN pour voir l'adresse MAC des différentes interface réseau

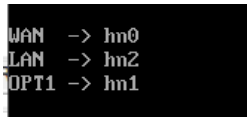


Je vais correspondre les différentes cartes réseaux aux interfaces WAN,LAN



Je fais correspondre ici

A la fin sa me donne ce résultat

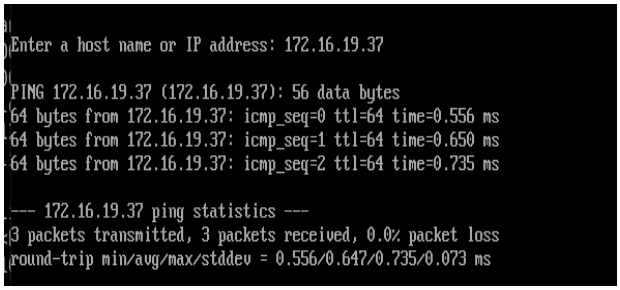


WAN = VLAN 60
LAN = VLAN 40
OPT1 = DMZ VLAN 30

L'IP attribuer en dhcp dans le vlan 60 au pare-feu est celle ci

172.16.19.35/24

Je vais essayer de pinger ma debian depuis le pfsense



Ça fonctionne

Le mot de passe par défaut sur pfsense est :

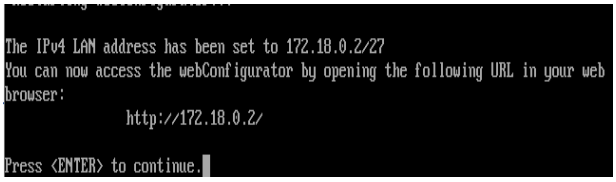
Login = admin
mdp = pfsense

Je dois accéder au pare feu depuis le LAN et non le WAN donc je lui attribue une ip dans le vlan 40 et j'attribue une IP de ma Debian aussi

IP dans vlan 40 = 172.18.0.2 (Toutes les ip de tout les TP sont dans le fichier excel)

IP dans vlan 30 =

Maintenant je peux accéder à l'interface web depuis la patte LAN

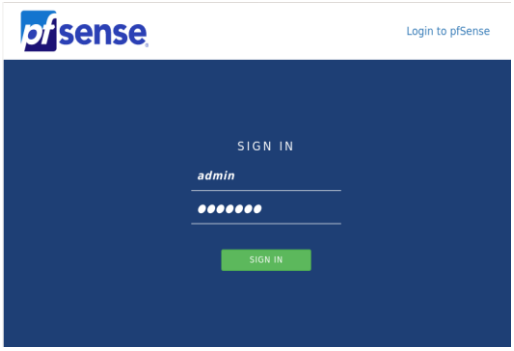


Je configure l'IP sur la 3 -ème patte LAN

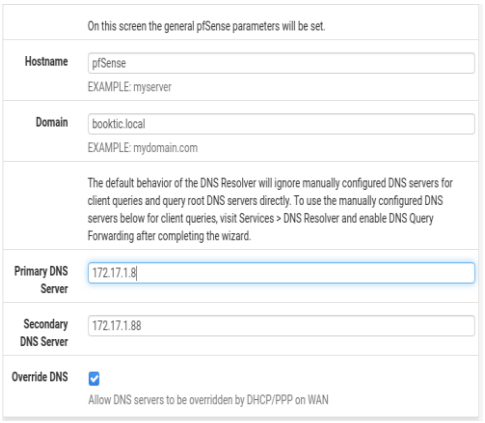
Ensuite je vais sur l'interface web du pare-feu et j'ai cette erreur

En tout cas j'arrive à contacter le serveur web mais il y'a une erreur ce n'est pas grave je vais m'informer

Je dois retourner dans le menu et choisir l'option 16 qui redémarre PHP

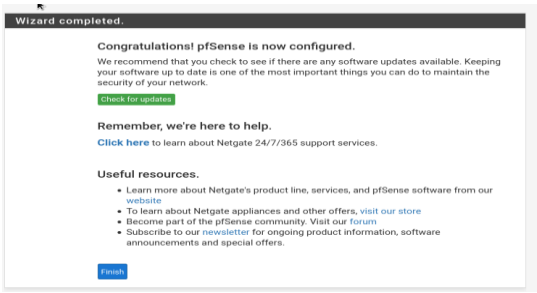


- Je me connecte
- Je configure le DNS



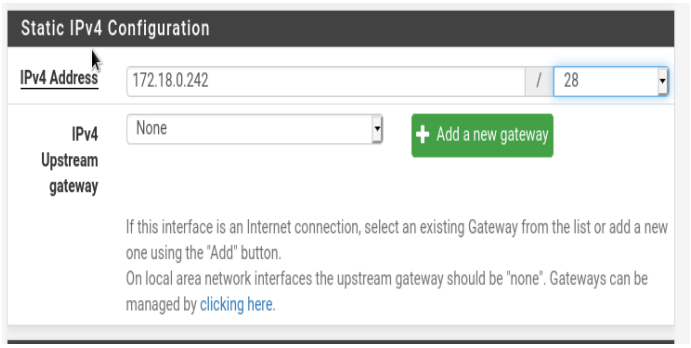
- Je modifie le fuseau horaire
- Je confirme les IP que j'avais déterminer en ligne de commande

Configuration de base terminer

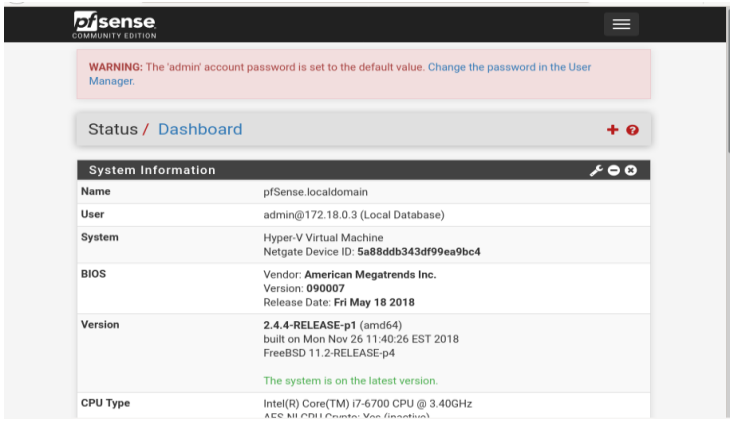


Me voilà dans l'interface d'administration

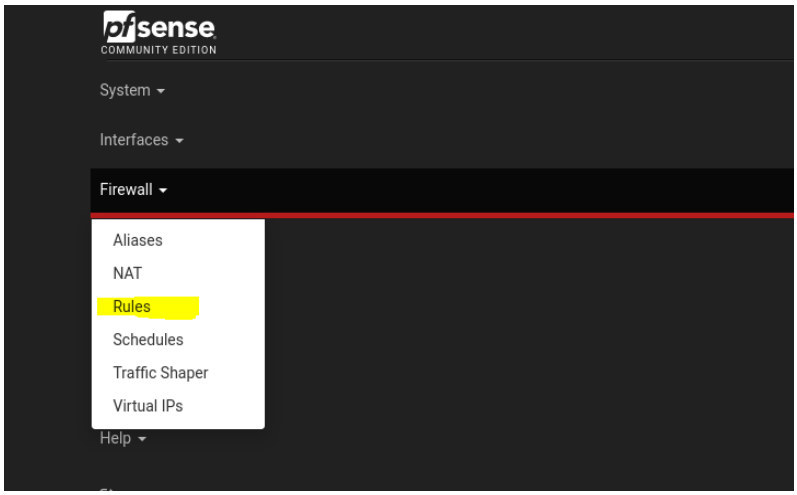
J'attribue l'IP du pare-feu dans le vlan 30 comme ceci



L’écran d’accueil



<u>Pour modifier les règles je vais dans l’onglet Rules</u>

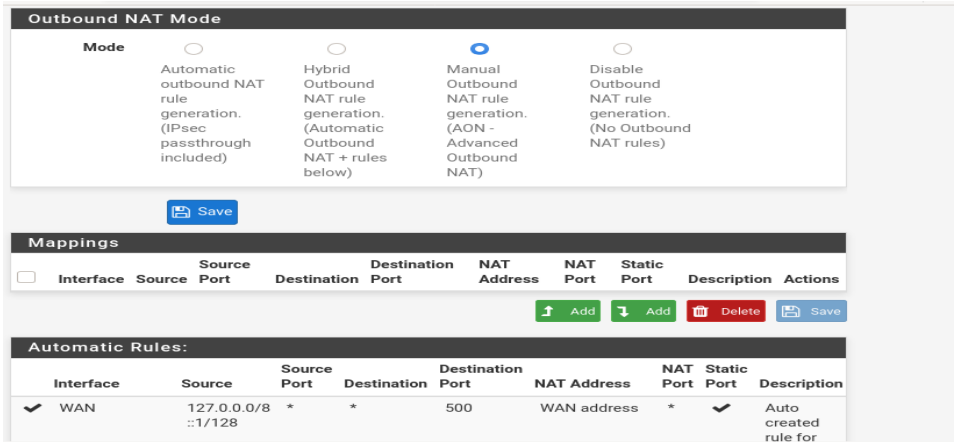


- Je renomme les interfaces d’abord
- L’interface WAN garde son nom
- l4interface LAN s’appellera désormais ADMINVLAN30
- L’interface OPT1 s’appellera DMZVLAN40

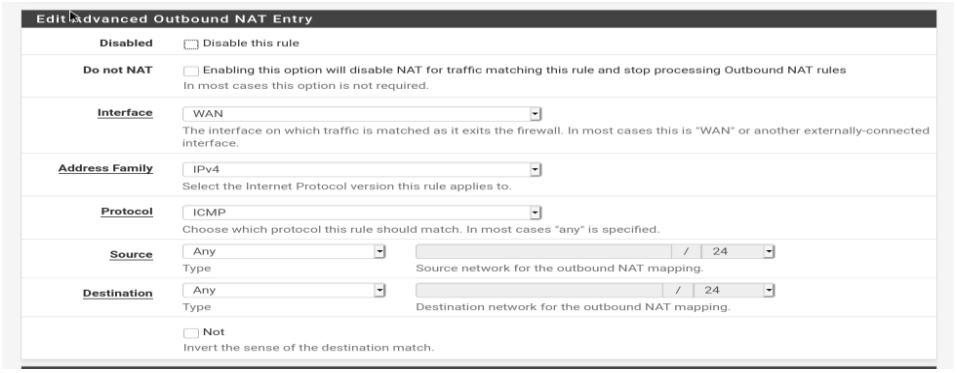
MISE EN PLACE DU NAT

Je vais dans /Firewall /NAT

Je choisis manuel outbound pour que ça soit moi qui configure les règles de Nat par défaut les règles sont créé automatiquement



Je configure la première règle de NAT pour le VLAN 30 ADMIN

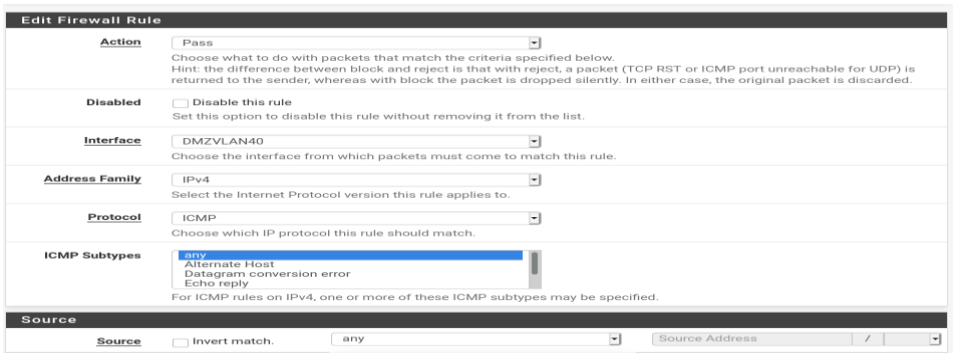


Je dis que toute IPV4 qui lance un ping vient de n'importe quel réseau interne

A destination de n'importe quel IP dans le WAN

Sera masquer par l'IP de l'interface WAN

Je dois aussi mettre une règle de pare feu qui autorise le ping sortant du VLAN 40 à destination du WAN



Et dans la destination j'ai mis ceci

J'ai mis WAN net

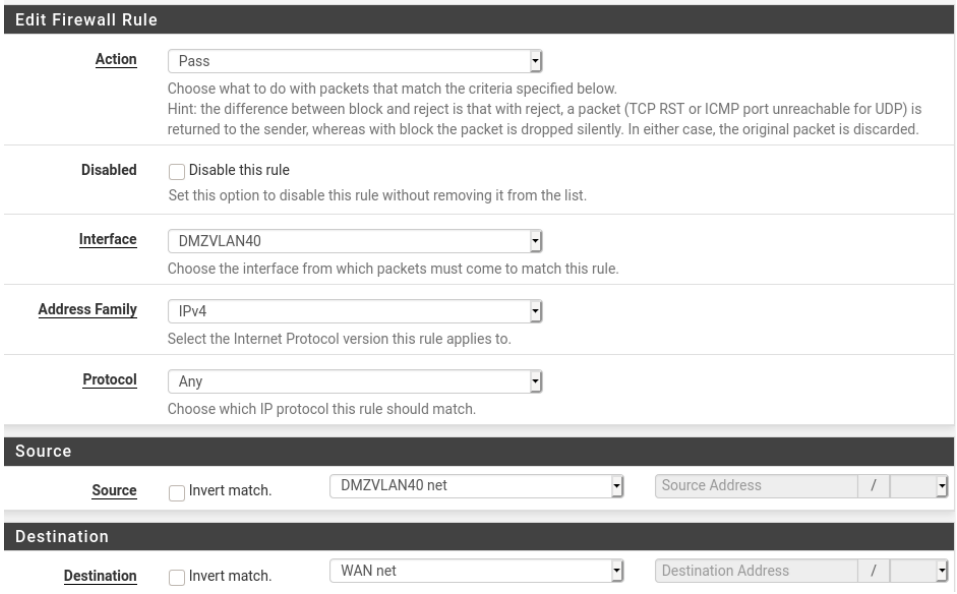
La différence entre WAN net et WAN address

WAN net = C'est toutes les ip qui sont dans le WAN hormis celle de mon pare feu dans le WAN

WAN address = C'est l'IP du routeur dans le WAN

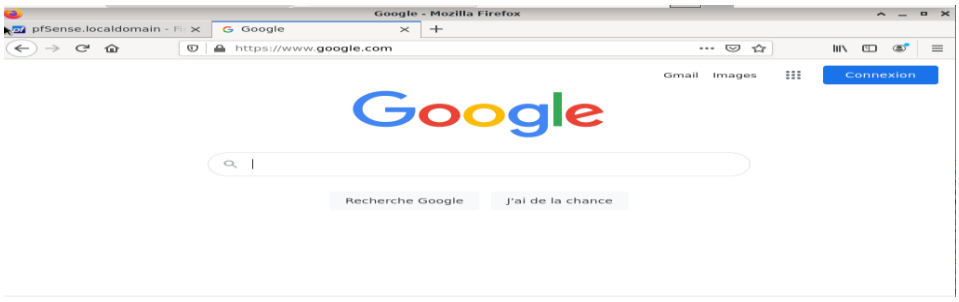
Il faut d'abord faire une règle de pare-feu qui autorise le trafic venant de l'interface intérieur LAN à traverser l'interface WAN pour envoyer des paquets à des machines dans le WAN

Maintenant que j'ai autoriser les pings depuis la DMZ vers le WAN j'autorise tout le trafic sortant de la DMZ à aller vers le WAN



Voici ma règle qui permet tout le trafic avec n'importe quel port source vers n'importe quel IP dans le LAN vers n'importe quel port destination en TCP et UDP

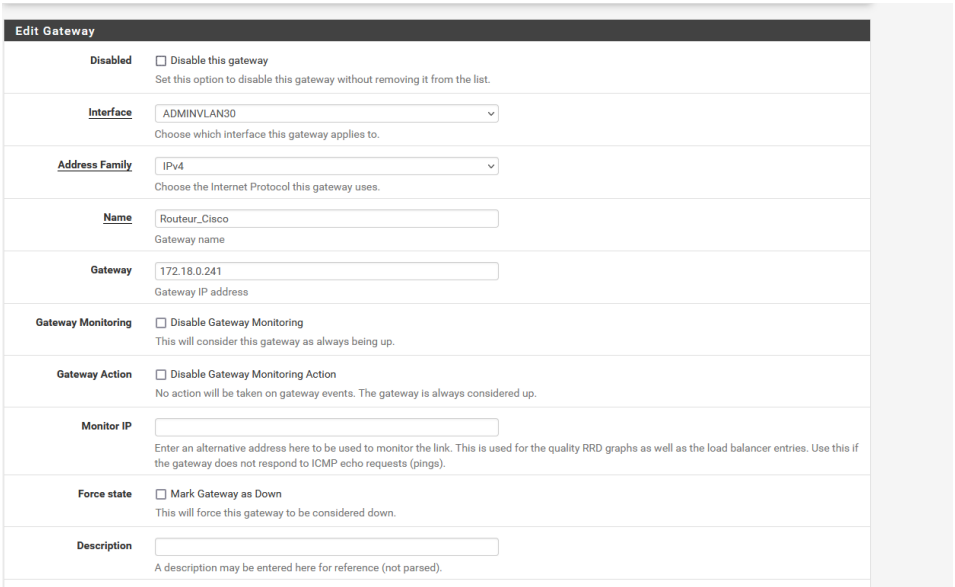
Je teste d'ouvrir mon navigateur et aller sur google



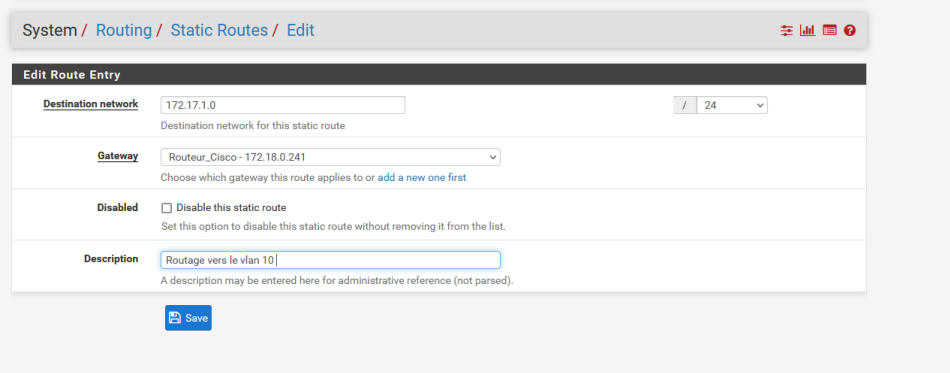
Ça fonctionne parfaitement

Mise en place des règles

- Je place ma deb 11 dans le vlan
- Je crée une route sur le pare feu pour qu'il puisse router vers le vlan 10 car il y'a mon proxy dedans
- Je vais dans
- System
- Routing
- Static Routes
- La destination sera le réseau du vlan 10
- L'interface sera l'IP du pare-feu dans le vlan 30 admin
- -La passerelle sera l'IP du routeur cisco dans le vlan 30
- D'abord je vais dans Gateway avant static routes
- Et je crée une nouvelle Gateway qui sera le routeur cisco dans le vlan 30



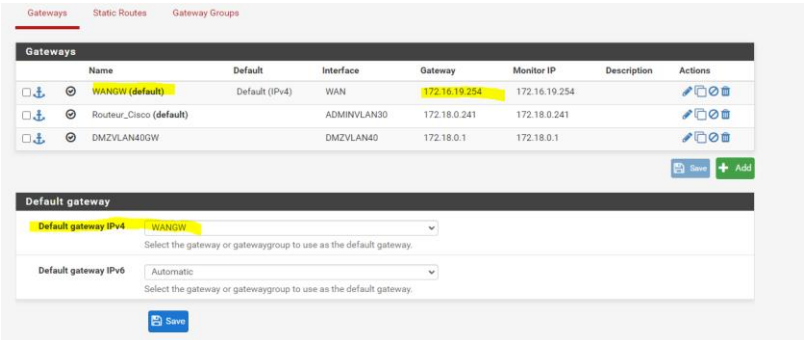
Je repars dans route (et je configure une route pour que mon pfsense puisse aller vers le vlan 10)



La route ressemble à sa

Ensuite je fais en sorte que la passerelle par défaut du pare-feu pfsense sois le routeur de la salle

Comme ceci



Pour que dès qu'il ne connaît pas le réseau de destination il passera par le routeur de la salle comme demander dans le TP

D'après ce que j'ai compris lorsque l'on définit une Gateway dans l'interface du pare feu pfsense ce n'est enfaite que la route par défaut
0.0.0.0 /0

Ensuite en ce qui concerne les Gateway que l'on peut configurer dans les interfaces si le réseau de l'interface est un LAN il faut mettre « none »

Et si le réseau de l'interface c'est le WAN la Gateway sera l'IP du prochain routeur à atteindre

Pour que tout fonctionne correctement il faut supp l'interface virtuel fa0/0.40 qui était dans la DMZ et créer une route pour atteindre le vlan40 qui est la DMZ cette route sera comme ceci

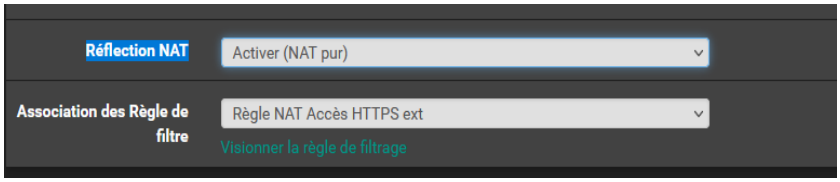
Destination = 172.18.0.0 /27
Interface = 172.18.0.1
Passerelle = 172.18.0.30

Soit sur une commande cisco
Ça ressemble à ceci = ip route 172.18.0.0 255.255.255.224 172.18.0.30

Ma part du travail sur pfsense est terminer je passe la main à gabriel qui va gérer les différentes règles du pare feu

Résolution du problème DNS rebind attack avec les règles de DNAT

Il faut que dans notre règle de DNAT paramétrer la reflection NAT en mode pur



Commenté [Auteur in1]: A la fin le routeur cisco pour atteindre la DMZ devra passer par le pare-feu pfsense car avant il y'avait 2 routeur et 2 Gateway différente dans la DMZ le routeur cisco qui faisait du routage inter-vlan et le pfsense derriere lui il y'avait la dmz les serveurs web

Maintenant avec cette modification il n'ya plus ce nœud et les paquets ne ce perdent plus entre 2 vlans qui ont le même nom mais un qui est dans un commutateur interne derrière le pfsense et un sur un commut externe qui servait au routage inter-vlan