

---

## Installation pfSense

---

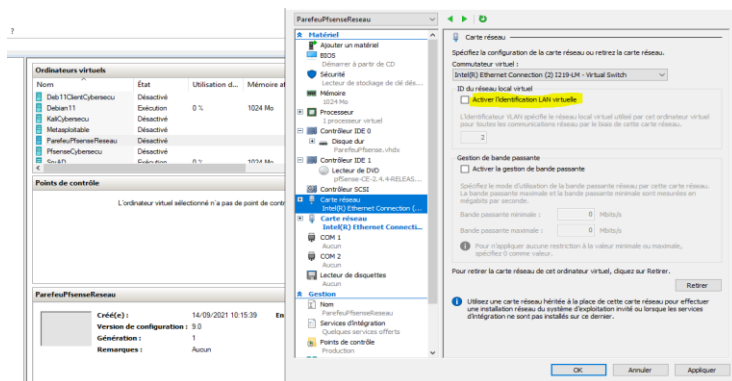
Il nous est demandé de brancher notre machine virtuelle dans 2 vlans via un port tagué

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

Une interface virtuelle comportant comme vlanID 60

Une deuxième interface virtuelle comportant comme vlanID 30

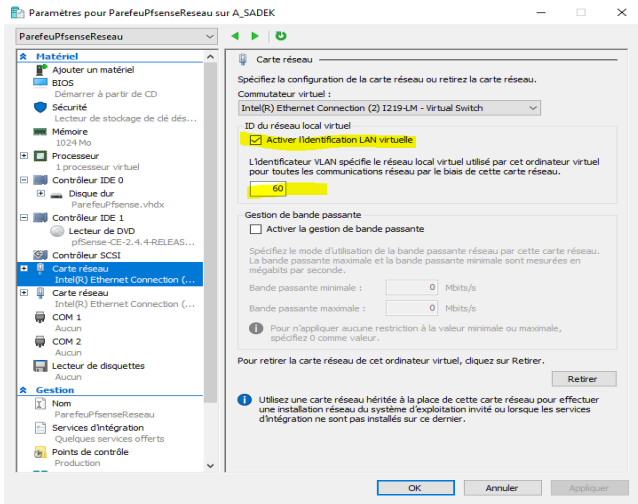
Et mes deux DMZ qui seront dans le vlan 40 mais dans un commutateur interne



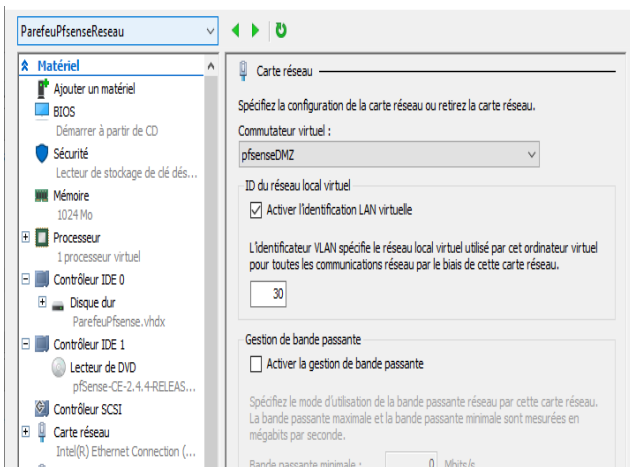
La première interface réseau est celle la

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

Et spécifier le vlan 60



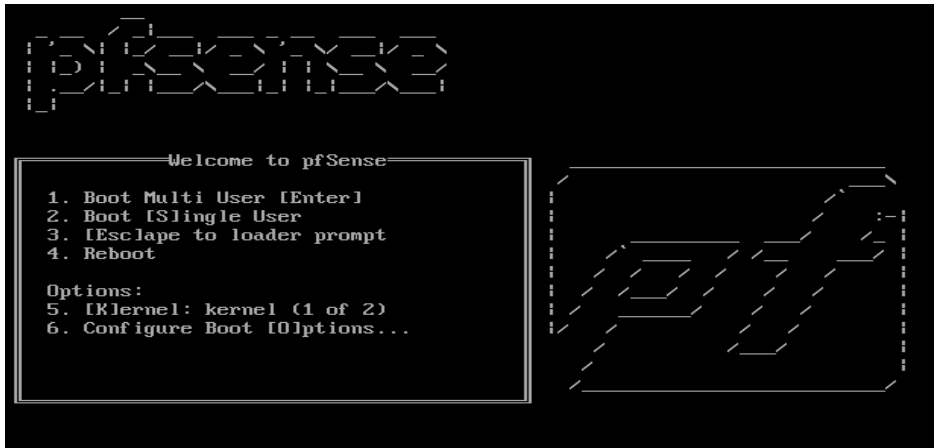
Et ici le commutateur interne



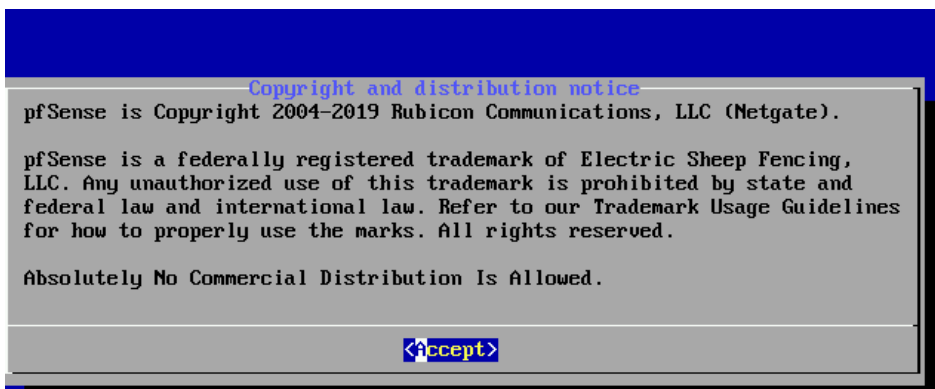
J'ai configuré les 3 interfaces comme ceci

Je lance la VM pfsense

L'écran d'installation s'affiche



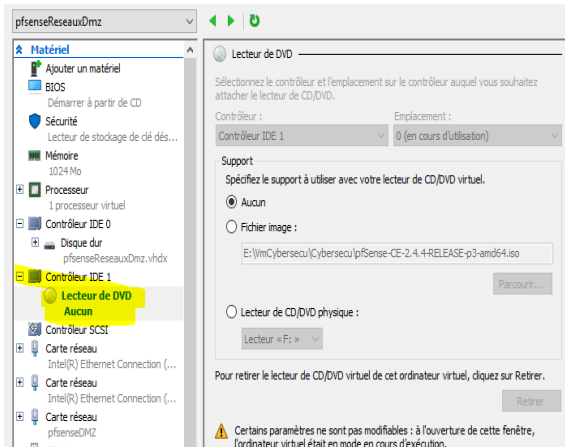
Je ne choisis rien je laisse sa ce lancera automatiquement



J'accepte

- Ensuite je sélectionne install pfsense
- Ensuite je choisis le clavier français et je lance une installation automatique
- Une fois l'installation terminée on me demande si je veux ouvrir un shell
- Je répond 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

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hm0 hm1 hm2 or a):
```

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

```
Carte réseau (MAC dynamique: 00:15:5D:13:1A:13) - Mode d'ac... Intel(R) Ether... fe80::215:5d... OK
Carte réseau (MAC dynamique: 00:15:5D:13:1A:14) - Mode d'ac... pfsenseDMZ fe80::215:5d... OK
Carte réseau (MAC dynamique: 00:15:5D:13:1A:12) - Mode d'ac... Intel(R) Ether... fe80::215:5d... OK
```

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

```

Valid interfaces are:
hm0      00:15:5d:13:1a:12 (down) Hyper-U Network Interface
hm1      00:15:5d:13:1a:13 (down) Hyper-U Network Interface
hm2      00:15:5d:13:1a:14 (up) Hyper-U Network Interface

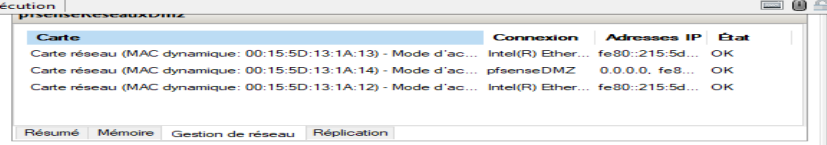
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]?
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hm0 hm1 hm2 or a):
Invalid interface name '1'

Enter the WAN interface name or 'a' for auto-detection
(hm0 hm1 hm2 or a):

```



Carte	Connexion	Adresses IP	État
Carte réseau (MAC dynamique: 00:15:5D:13:1A:13) - Mode d'ac...	Intel(R) Ether...	fe80::2155d...	OK
Carte réseau (MAC dynamique: 00:15:5D:13:1A:14) - Mode d'ac...	pfSenseDMZ	0.0.0.0, fe8...	OK
Carte réseau (MAC dynamique: 00:15:5D:13:1A:12) - Mode d'ac...	Intel(R) Ether...	fe80::2155d...	OK

Je fais correspondre ici

A la fin sa me donne ce résultat

```

WAN -> hm0
LAN -> hm2
OPT1 -> hm1

```

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

```

*** welcome to pfSense 2.7.1 RELEASE (amd64) on pfSense ***

WAN (wan)      -> hm0      -> v4/DHCP4: 172.16.19.35/24
LAN (lan)      -> hm2      ->
OPT1 (opt1)    -> hm1      ->

```

**172.16.19.35/24**

Je vais essayer de pinguer ma debian depuis le pfSense

```
Enter a host name or IP address: 172.16.19.37
PING 172.16.19.37 (172.16.19.37): 56 data bytes
64 bytes from 172.16.19.37: icmp_seq=0 ttl=64 time=0.556 ms
64 bytes from 172.16.19.37: icmp_seq=1 ttl=64 time=0.650 ms
64 bytes from 172.16.19.37: icmp_seq=2 ttl=64 time=0.735 ms
--- 172.16.19.37 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.556/0.647/0.735/0.073 ms
```

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

```
The IPv4 LAN address has been set to 172.18.0.2/27
You can now access the webConfigurator by opening the following URL in your web browser:
      http://172.18.0.2/
Press <ENTER> to continue.
```

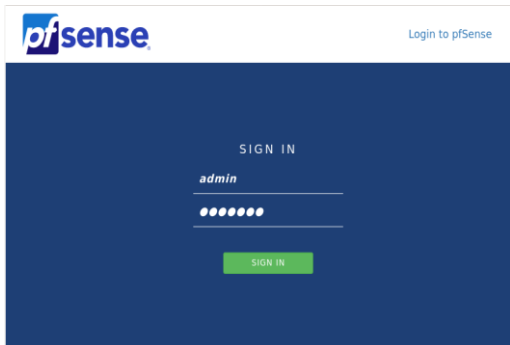
Je configure l'IP sur la 3 -ème patte LAN

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

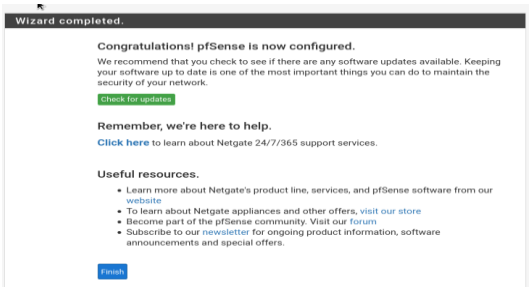


- Je me connecte
- Je configure le DNS

On this screen the general pfSense parameters will be set.	
Hostname	<input type="text" value="pfSense"/> <small>EXAMPLE: myserver</small>
Domain	<input type="text" value="booktic.local"/> <small>EXAMPLE: mydomain.com</small>
<p>The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services &gt; DNS Resolver and enable DNS Query Forwarding after completing the wizard.</p>	
Primary DNS Server	<input type="text" value="172.17.1.8"/>
Secondary DNS Server	<input type="text" value="172.17.1.88"/>
Override DNS	<input checked="" type="checkbox"/> <small>Allow DNS servers to be overridden by DHCP/PPP on WAN</small>

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

## Configuration de base terminer



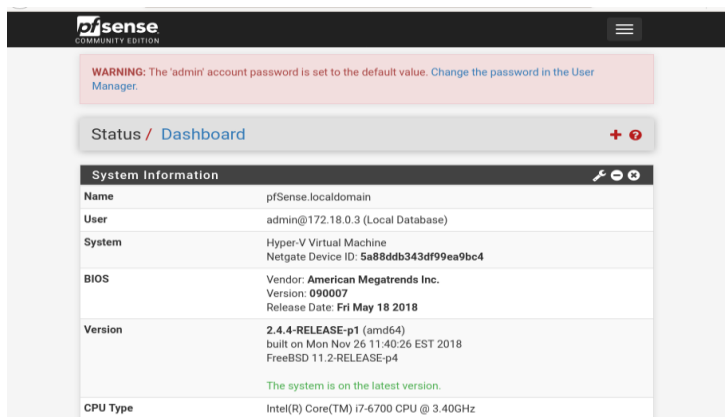
Me voilà dans l'interface d'administration

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

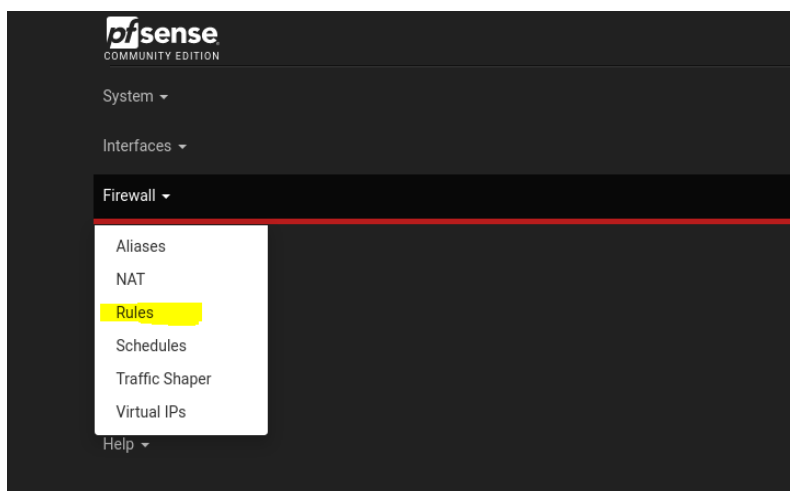




## L'écran d'accueil



## Pour modifier les règles je vais dans l'onglet Rules



- Je renomme les interfaces d'abord
- L'interface WAN garde son nom
- l'interface 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

The screenshot shows the Mikrotik WinBox NAT configuration interface. At the top, the "Outbound NAT Mode" section has four radio buttons: "Automatic outbound NAT rule generation. (IPsec passthrough included)", "Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)", "Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)", and "Disable Outbound NAT rule generation. (No Outbound NAT rules)". The "Manual" option is selected. Below this is a "Save" button. The "Mappings" section is a table with columns: Interface, Source, Source Port, Destination, Destination Port, NAT Address, NAT Port, Static Port, Description, and Actions. Below the table are "Add" (up arrow), "Add" (down arrow), "Delete", and "Save" buttons. The "Automatic Rules:" section contains a table with columns: Interface, Source, Source Port, Destination, Destination Port, NAT Address, NAT Port, Static Port, and Description. One rule is listed for the WAN interface with source 127.0.0.0/8 ::1/128, destination \*, destination port 500, NAT address WAN address, NAT port \*, and static port checked. Description: Auto created rule for

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

The screenshot shows the "Edit Advanced Outbound NAT Entry" configuration window. It includes several sections: "Disabled" with a checkbox "Disable this rule"; "Do not NAT" with a checkbox "Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required."; "Interface" set to "WAN" with a dropdown; "Address Family" set to "IPv4" with a dropdown; "Protocol" set to "ICMP" with a dropdown; "Source" with "Any" selected, "Type" dropdown, and "Source network for the outbound NAT mapping." field; "Destination" with "Any" selected, "Type" dropdown, and "Destination network for the outbound NAT mapping." field; and a "Not" checkbox with the label "Invert the sense of the destination match."

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

**Edit Firewall Rule**

**Action**  Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface**   
Choose the interface from which packets must come to match this rule.

**Address Family**   
Select the Internet Protocol version this rule applies to.

**Protocol**   
Choose which IP protocol this rule should match.

**ICMP Subtypes**   
any  
Alternate Host  
Datagram conversion error  
Echo reply  
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**Source**

**Source**  Invert match.  Source Address /

Et dans la destination j'ai mis ceci

**Source**

**Source**  Invert match.  Source Address /

**Destination**

**Destination**  Invert match.  Destination Address /

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 autorisé les pings depuis la DMZ vers le WAN j'autorise tout le trafic sortant de la DMZ à aller vers le WAN**

**Edit Firewall Rule**

**Action**    
 Choose what to do with packets that match the criteria specified below.   
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule   
 Set this option to disable this rule without removing it from the list.

**Interface**    
 Choose the interface from which packets must come to match this rule.

**Address Family**    
 Select the Internet Protocol version this rule applies to.

**Protocol**    
 Choose which IP protocol this rule should match.

**Source**

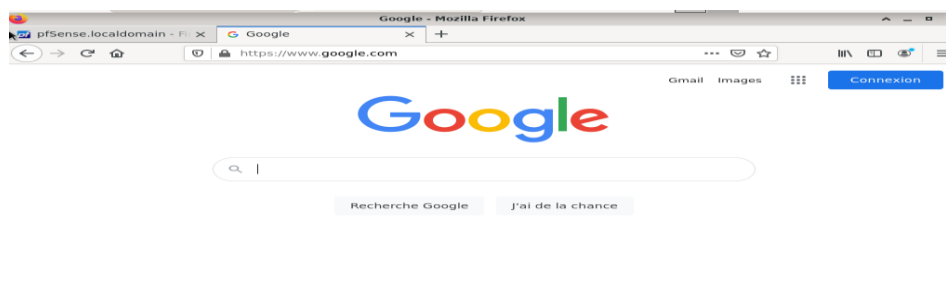
**Source**  Invert match.   /

**Destination**

**Destination**  Invert match.   /

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

Edit Gateway	
<b>Disabled</b>	<input type="checkbox"/> Disable this gateway Set this option to disable this gateway without removing it from the list.
<b>Interface</b>	ADMINVLAN30 Choose which interface this gateway applies to.
<b>Address Family</b>	IPv4 Choose the Internet Protocol this gateway uses.
<b>Name</b>	Routeur_Cisco Gateway name
<b>Gateway</b>	172.18.0.241 Gateway IP address
<b>Gateway Monitoring</b>	<input type="checkbox"/> Disable Gateway Monitoring This will consider this gateway as always being up.
<b>Gateway Action</b>	<input type="checkbox"/> Disable Gateway Monitoring Action No action will be taken on gateway events. The gateway is always considered up.
<b>Monitor IP</b>	<input type="text"/> Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
<b>Force state</b>	<input type="checkbox"/> Mark Gateway as Down This will force this gateway to be considered down.
<b>Description</b>	<input type="text"/> A description may be entered here for reference (not parsed).

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

System / Routing / Static Routes / Edit

**Edit Route Entry**

**Destination network** 172.17.1.0 / 24  
Destination network for this static route

**Gateway** Routeur\_Cisco - 172.18.0.241  
Choose which gateway this route applies to or [add a new one first](#)

**Disabled**  Disable this static route  
Set this option to disable this static route without removing it from the list.

**Description** Routeage vers le vlan 10  
A description may be entered here for administrative reference (not parsed).

[Save](#)

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

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
WANGW (default)	Default (IPv4)	WAN	172.16.19.254	172.16.19.254		<a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>
Routeur_Cisco (default)		ADMINVLAN30	172.18.0.241	172.18.0.241		<a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>
DMZVLAN40GW		DMZVLAN40	172.18.0.1	172.18.0.1		<a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>

**Default gateway**

**Default gateway IPv4** WANGW  
Select the gateway or gatewaygroup to use as the default gateway.

**Default gateway IPv6** Automatic  
Select the gateway or gatewaygroup to use as the default gateway.

[Save](#)

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

<b>Réflexion NAT</b>	Activer (NAT pur) ▼
Association des Règle de filtre	Règle NAT Accès HTTPS ext ▼ <a href="#">Visionner la règle de filtrage</a>

**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 derriere le pfsense et un sur un commut externe qui servait au routage inter-vlan

