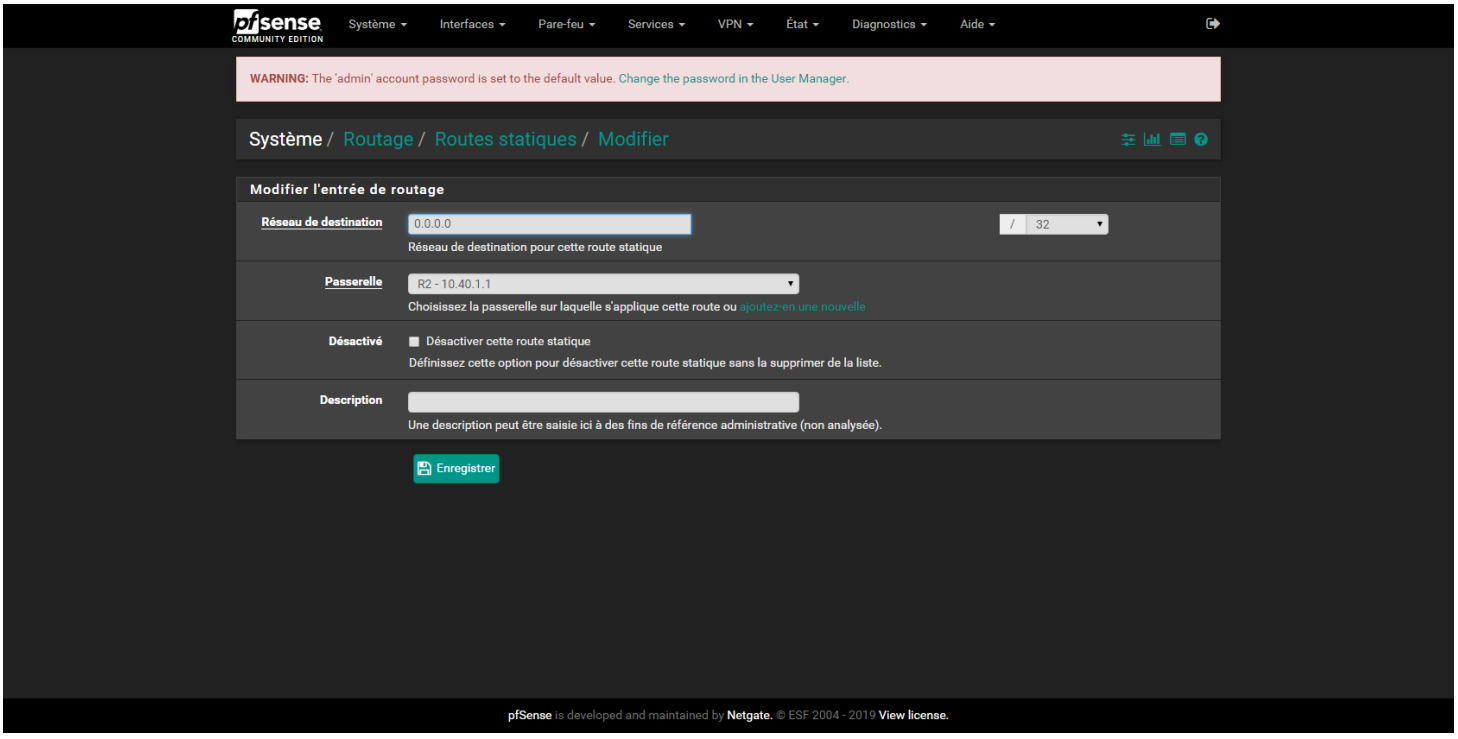
SISR5 – FIREWALL

I. Accès web depuis le LAN (ICMP + http)

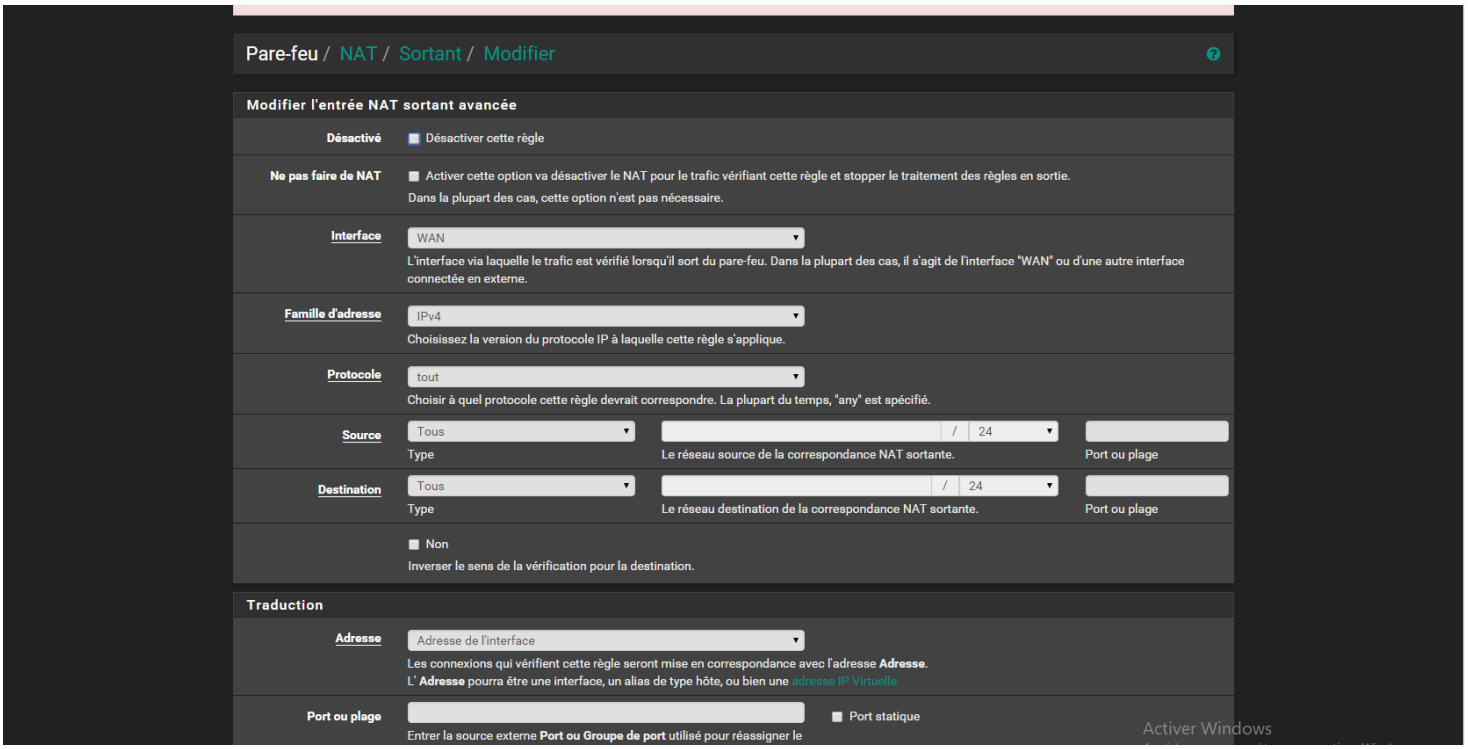
Pour commencer, nous avons besoin de créer une route par défaut afin de diriger les requêtes du LAN d'accéder au WAN (et donc internet).

Voici la configuration :



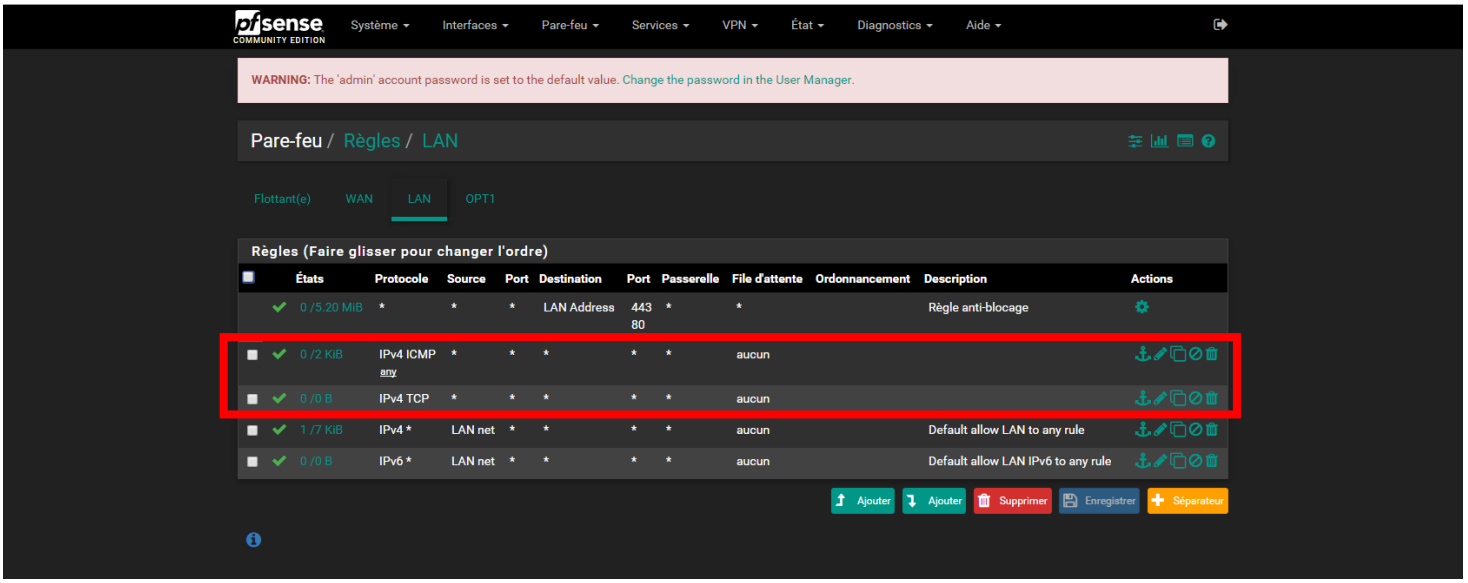
Nous indiquons donc dans « Réseau de destination » l'adresse IP : 0.0.0.0 avec le masque /32 (CIDR). Afin nous indiquons que la passerelle est la routeur R2, donc 10.40.1.1.

Une fois cela fait passons à présent à la translation d'adresse. Pour se faire direction le NAT dans les réglages du pare-feu. Ensuite dans l'onglet « Sortant », ajouter une nouvelle règle comme ceci :



Choisir l'interface WAN, indiquer vouloir autoriser tous les protocoles. De même sur la source et la destination, on laisse vide les champs des adresses IP afin de tout autoriser.

Au niveau des règles du pare-feu, onglet LAN, voici ce qu'il faut ajouter ensuite :



Il s'agit de deux règles permettant de lui indiquer qu'il doit laisser passer les trames ICMP et TCP provenant de n'importe quelle source en direction de n'importe quelle destination et de

n'importe quel port.
Afin de justifier que les trames passent correctement à travers le FireWall, voici quelques preuves :

AVANT LE PARE-FEU

*- [PFSense-1 Ethernet0 to IOU2 Ethernet0/0]

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	aa:bb:cc:00:02:00	Spanning-tree-(for-…	STP	60	RST. Root = 32768/1/aa:bb:cc:00:02:00 Cost = 0 Port = 0x8001
2	0.219729	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request id=0x3f1d, seq=232/59392, ttl=64 (reply in 3)
3	0.220275	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply id=0x3f1d, seq=232/59392, ttl=255 (request in 2)
4	0.747594	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request id=0x3f1d, seq=233/59648, ttl=64 (reply in 5)
5	0.748159	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply id=0x3f1d, seq=233/59648, ttl=255 (request in 4)
6	1.276599	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request id=0x3f1d, seq=234/59904, ttl=64 (reply in 7)
7	1.277095	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply id=0x3f1d, seq=234/59904, ttl=255 (request in 6)
8	1.818720	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request id=0x3f1d, seq=235/60160, ttl=64 (reply in 9)
9	1.819302	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply id=0x3f1d, seq=235/60160, ttl=255 (request in 8)

APRES LE PARE-FEU

*- [IOU1 Ethernet0/1 to PFSense-1 Ethernet2]

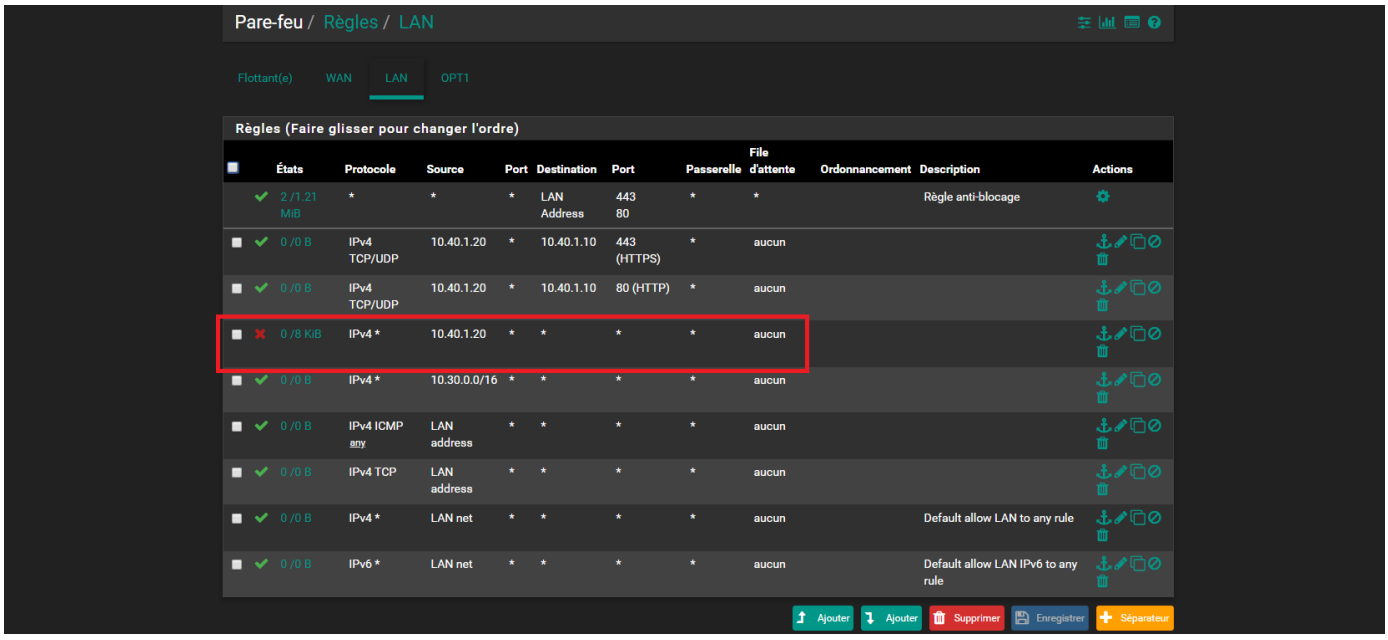
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4	0.400109	aa:bb:cc:00:01:10	Spanning-tree-(for-…	STP	60	RST. Root = 32768/1/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8002
5	0.676500	50.1.1.1	50.1.1.10	ICMP	42	Echo (ping) request id=0x5654, seq=311/14081, ttl=64 (reply in 6)
6	0.677375	50.1.1.10	50.1.1.1	ICMP	42	Echo (ping) reply id=0x5654, seq=311/14081, ttl=128 (request in 5)
7	1.046363	50.1.1.1	199.7.83.42	DNS	70	Standard query 0xbe49 NS <Root> OPT
8	1.219119	50.1.1.1	50.1.1.10	ICMP	42	Echo (ping) request id=0x5654, seq=312/14337, ttl=64 (reply in 9)
9	1.220241	50.1.1.10	50.1.1.1	ICMP	42	Echo (ping) reply id=0x5654, seq=312/14337, ttl=128 (request in 8)
10	1.746448	50.1.1.1	50.1.1.10	ICMP	42	Echo (ping) request id=0x5654, seq=313/14593, ttl=64 (reply in 11)
11	1.747204	50.1.1.10	50.1.1.1	ICMP	42	Echo (ping) reply id=0x5654, seq=313/14593, ttl=128 (request in 10)
12	2.275230	50.1.1.1	50.1.1.10	ICMP	42	Echo (ping) request id=0x5654, seq=314/14849, ttl=64 (reply in 13)
13	2.275868	50.1.1.10	50.1.1.1	ICMP	42	Echo (ping) reply id=0x5654, seq=314/14849, ttl=128 (request in 12)

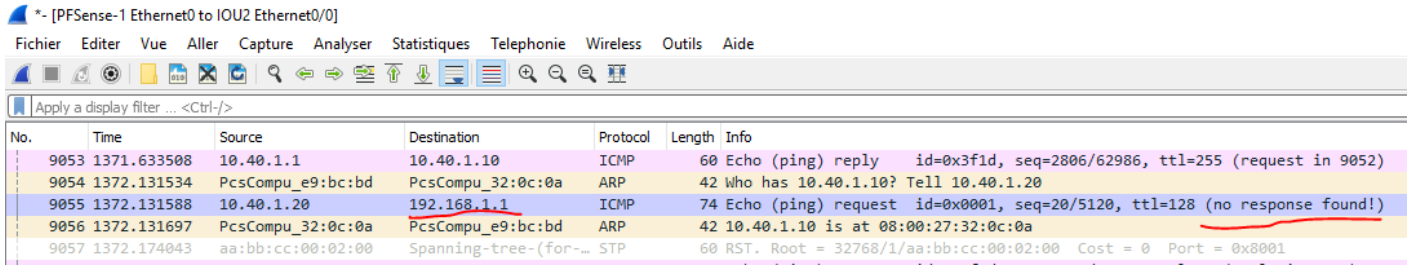
II. Bloquer l'accès web au PCConfig

Afin que le poste « PCConfig » n'accède plus à internet, il faut créer 2 nouvelles règles dans le pare-feu indiquant que les trames de ping (ICMP) ainsi que celle en direction des ports 80 (http) et 443 (https) ne doivent pas passer.

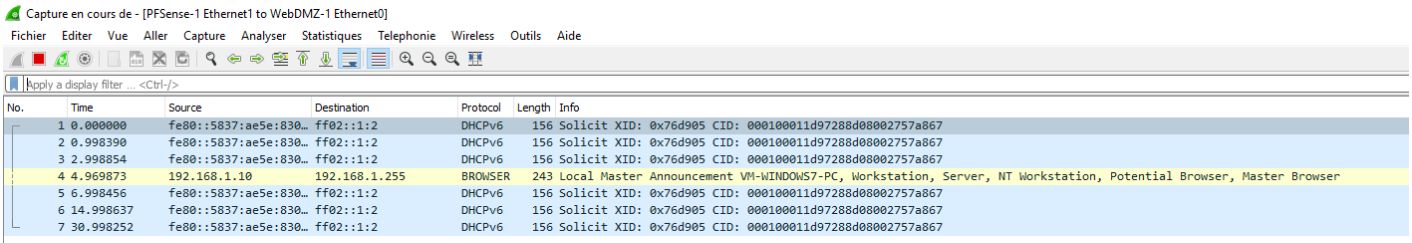


Afin de justifier que le PC n'a plus accès à internet voici quelques trames d'avant et après le FireWall :

AVANT LE PARE-FEU



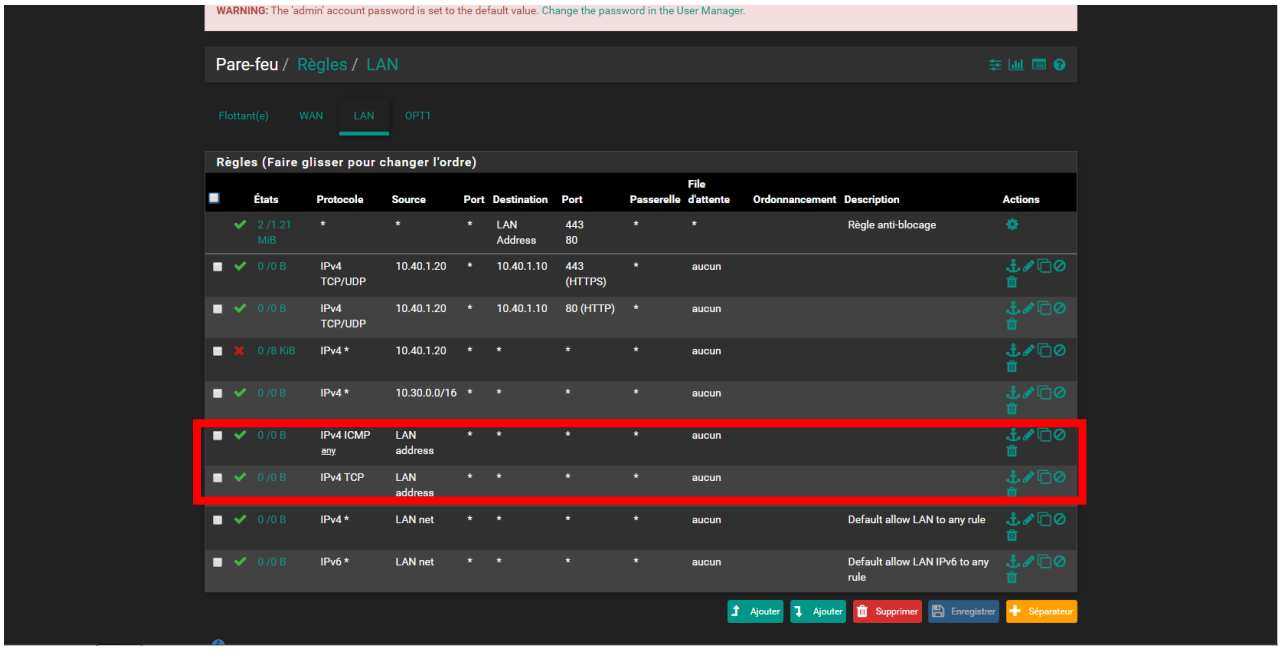
APRES LE PARE-FEU



On peut voir que la trame à destination de 192.168.1.1 ne passe pas à travers le FireWall. Sur la capture d'écran d'après le FireWall, on ne voit donc aucune trace de la trame.

III. Accès DMZ depuis l'intérieur (LAN)

Afin que le réseau LAN puisse avoir accès à la DMZ nous devons créer de nouvelles règles afin de lui permettre d'y accéder. Nous indiquons en source LAN address afin d'inclure toutes les adresses du réseau LAN et au niveau des ports et de la destination, nous laissons passer partout. Grâce à ces règles, le réseau LAN aura donc forcément accès à la DMZ.



IV. Masquage des adresses IP

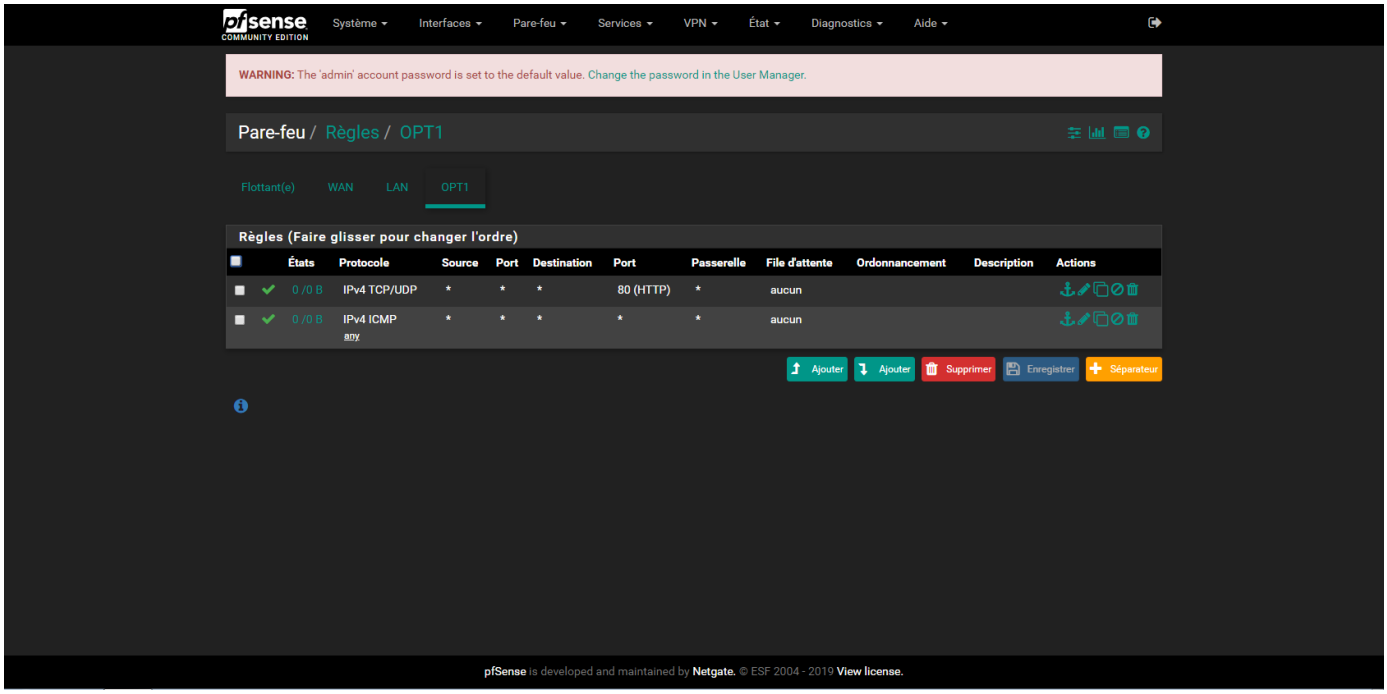
Voici les tests concluant sur le masquage de l'adresse IP :

```
7977 1808.820089   10.40.1.10      10.40.1.1       ICMP   42 Echo (ping) request  id=0x4059, seq…
7978 1808.820590   10.40.1.1       10.40.1.10      ICMP   60 Echo (ping) reply    id=0x4059, seq…
7979 1809.163811   10.30.1.10      192.168.1.10    ICMP   74 Echo (ping) request  id=0x0001, seq…
7980 1809.164360   192.168.1.10    10.30.1.10      ICMP   74 Echo (ping) reply    id=0x0001, seq…
7981 1809.362336   10.40.1.10      10.40.1.1       ICMP   42 Echo (ping) request  id=0x4059, seq…
7982 1809.371865   10.40.1.1       10.40.1.10      ICMP   60 Echo (ping) reply    id=0x4059, seq…
7983 1809.900841   10.40.1.10      10.40.1.1       ICMP   42 Echo (ping) request  id=0x4059, seq…
```

```
 244 1665.425350   192.168.1.1     192.168.1.10    ICMP   74 Echo (ping) request  id=0x60c5, seq…
 245 1665.426253   192.168.1.10    192.168.1.1     ICMP   74 Echo (ping) reply    id=0x60c5, seq…
 246 1666.425931   192.168.1.1     192.168.1.10    ICMP   74 Echo (ping) request  id=0x60c5, seq…
 247 1666.426140   192.168.1.10    192.168.1.1     ICMP   74 Echo (ping) reply    id=0x60c5, seq…
 248 1667.426869   192.168.1.1     192.168.1.10    ICMP   74 Echo (ping) request  id=0x60c5, seq…
```

V. Accès DMZ depuis l'extérieur

Pour pouvoir accéder à Internet depuis l'extérieur, nous avons besoin de faire un transfert de port (PAT). Pour se faire il faut ajouter deux règles sur le port OPT1.
La première permet de rediriger le port 80 et la deuxième permet de laisser passer toutes les trames pour ping un utilisateur.



Afin de justifier tout cela, voici une preuve via la commande ***tracert*** dans l'invite de commande Windows.