# Chapitre 1 – B2 – Epreuve E5 et expression des besoins

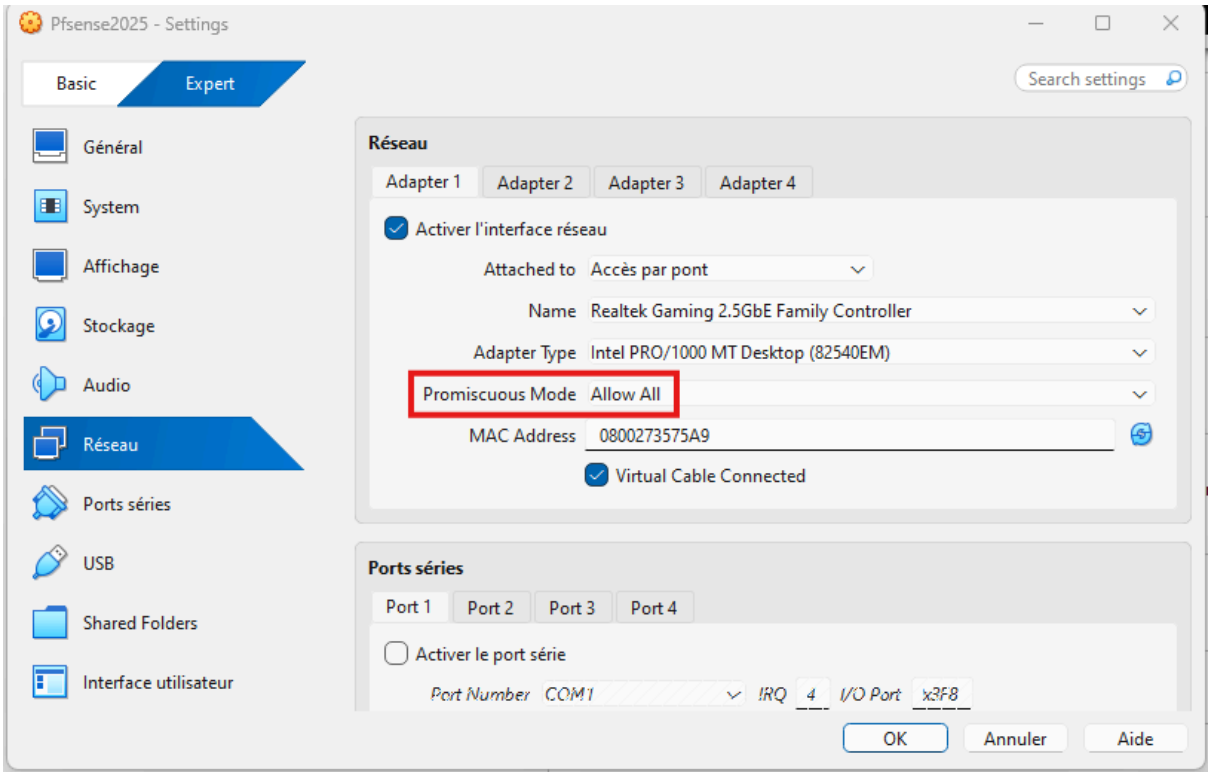
## Table des Matières :

```
pfSense 2.8.1-RELEASE amd64 20251024-1553
Bootup complete

FreeBSD/amd64 (pfSense.sio-exupery.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: c7050fd41dfe970d46bc

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

 WAN (wan)   -> em0 -> v4: 192.168.1.101/24
 LAN (lan)   -> em2 -> v4: 192.168.3.254/24
 OPT1 (opt1) -> em1 -> v4: 192.168.2.254/24
 OPT2 (opt2) -> em3 -> v4: 192.168.4.1/24

 0) Logout / Disconnect SSH           9) pfTop
 1) Assign Interfaces                10) Filter Logs
 2) Set interface(s) IP address      11) Restart GUI
 3) Reset admin account and password 12) PHP shell + pfSense tools
 4) Reset to factory defaults        13) Update from console
 5) Reboot system                    14) Enable Secure Shell (sshd)
 6) Halt system                      15) Restore recent configuration
 7) Ping host                        16) Restart PHP-FPM
 8) Shell

Enter an option:
```

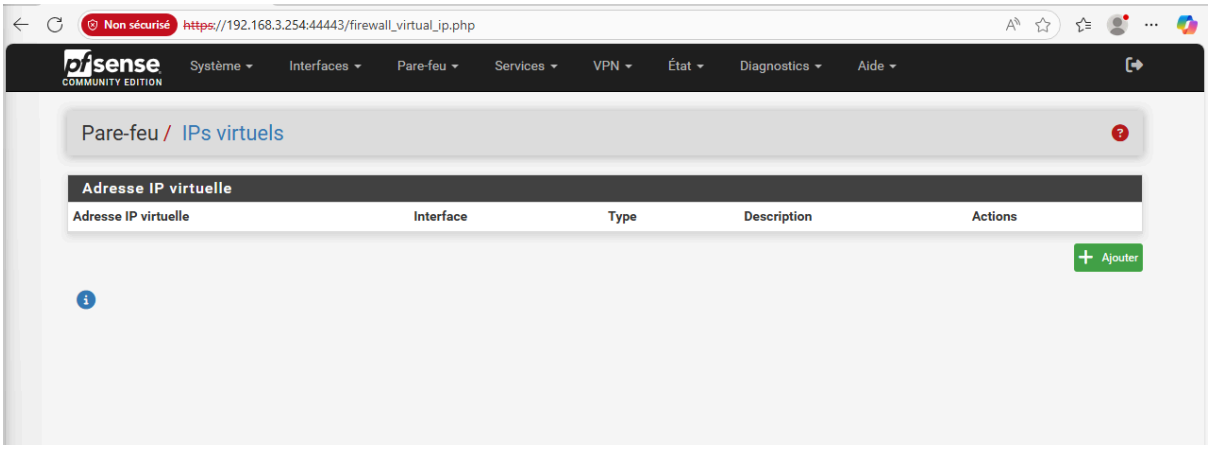
```
pfSense 2.8.1-RELEASE amd64 20251024-1553
Bootup complete

FreeBSD/amd64 (pfSense.sio-exupery.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 8993f0b9688f1652c472

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

 WAN (wan)   -> em0 -> v4: 192.168.1.102/24
 LAN (lan)   -> em2 -> v4: 192.168.3.254/24
 OPT1 (opt1) -> em1 -> v4: 192.168.2.254/24
 OPT2 (opt2) -> em3 -> v4: 192.168.4.2/24

 0) Logout / Disconnect SSH           9) pfTop
 1) Assign Interfaces                10) Filter Logs
 2) Set interface(s) IP address      11) Restart GUI
 3) Reset admin account and password 12) PHP shell + pfSense tools
 4) Reset to factory defaults        13) Update from console
 5) Reboot system                    14) Enable Secure Shell (sshd)
 6) Halt system                      15) Restore recent configuration
 7) Ping host                        16) Restart PHP-FPM
 8) Shell

Enter an option:
```

# MISSION1

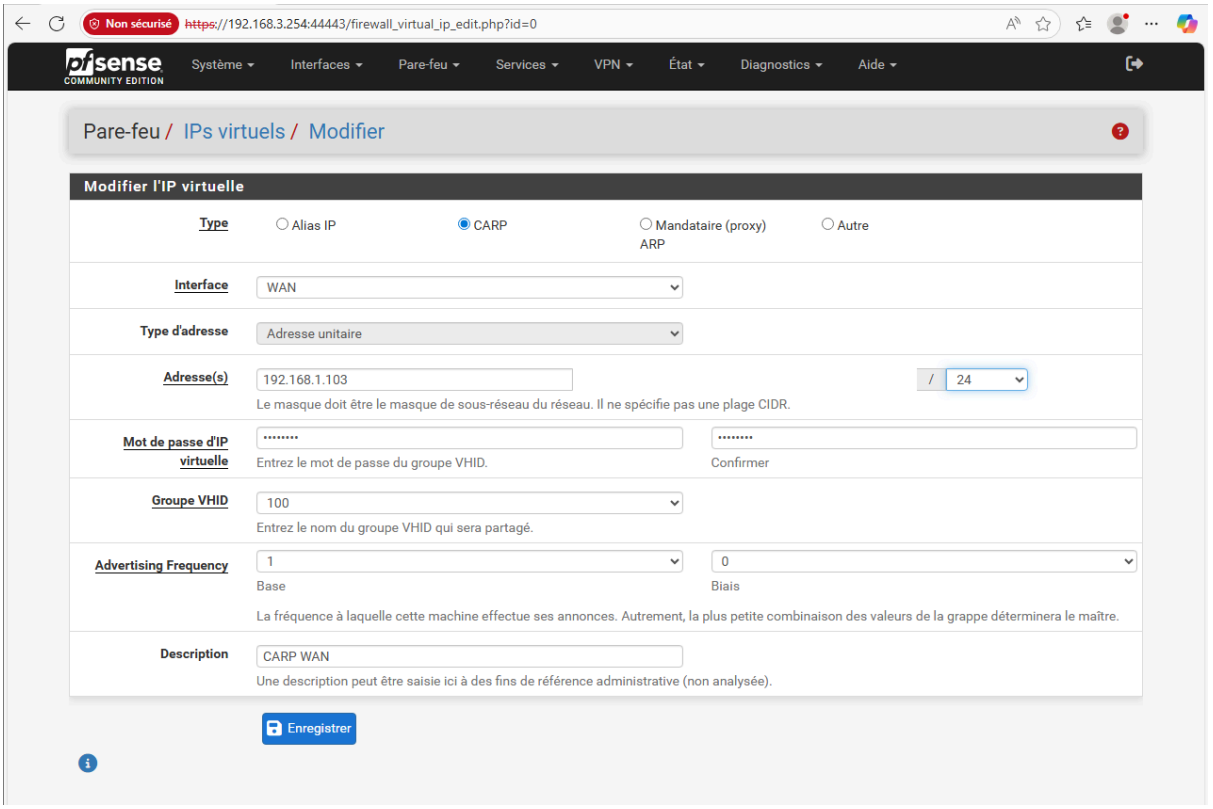
▪ Pour toutes les cartes des VM :

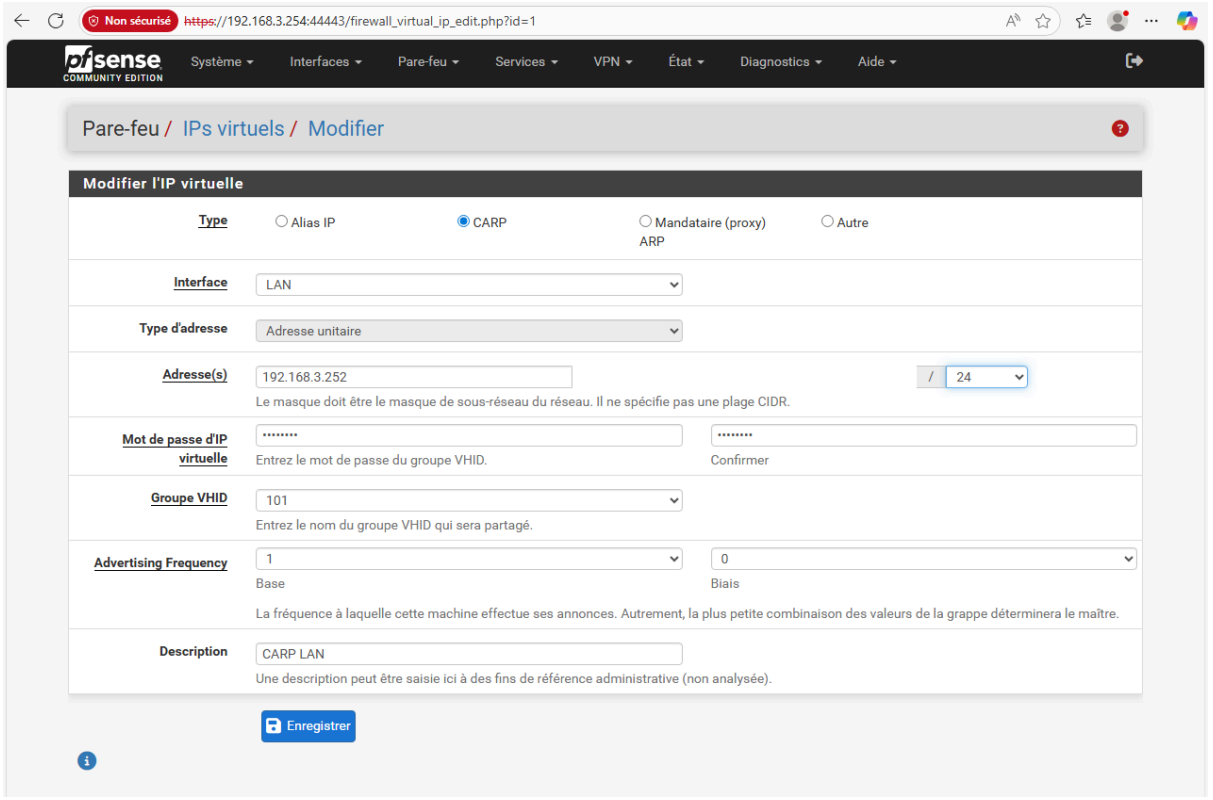


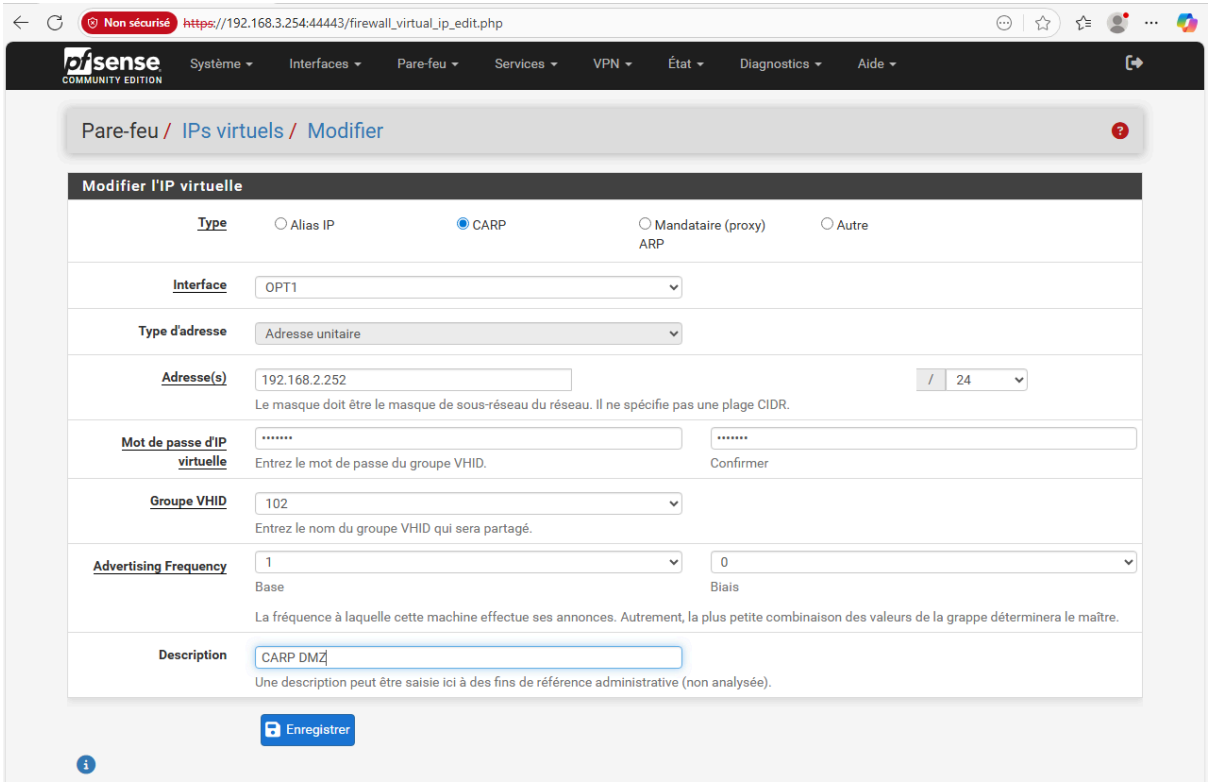

▪ Nous supprimons les éventuelles anciennes IP virtuelles :

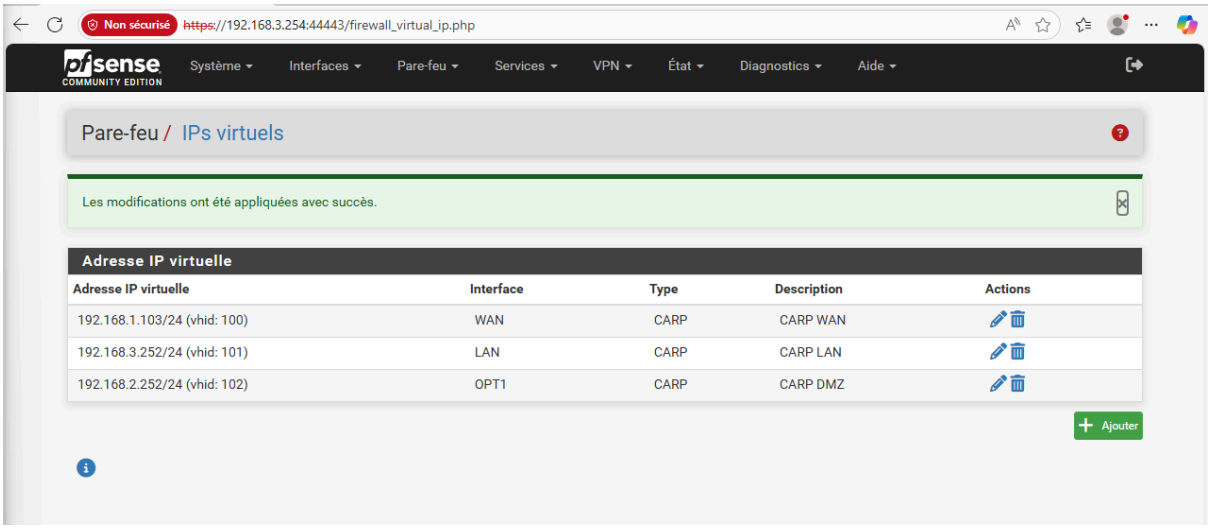


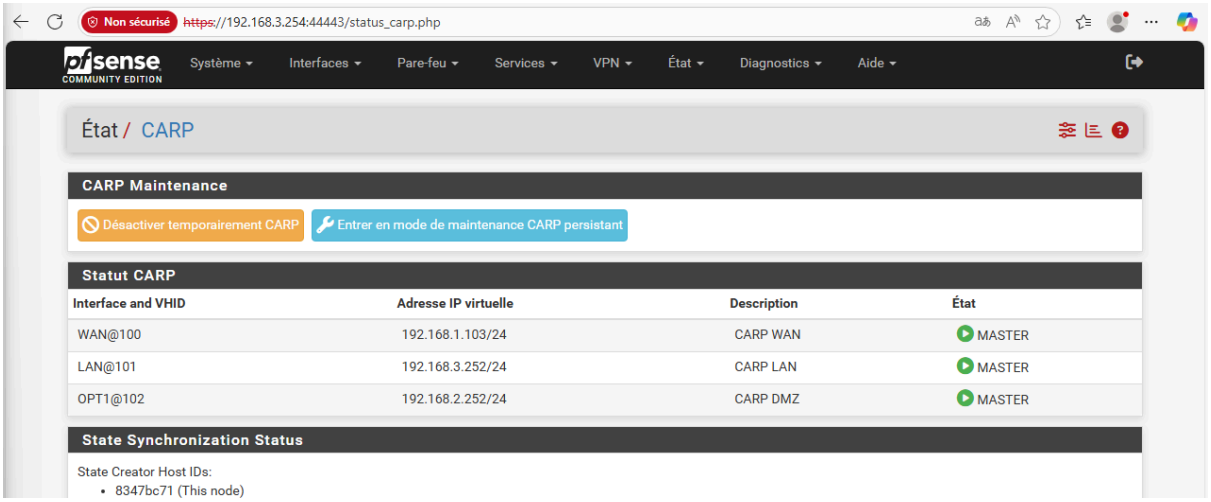
- Sur le pfsense Master :
  - Nous créons les VIP (CARP) pour chaque interface :

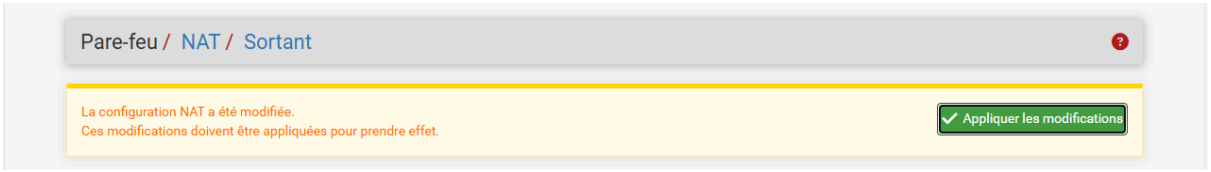


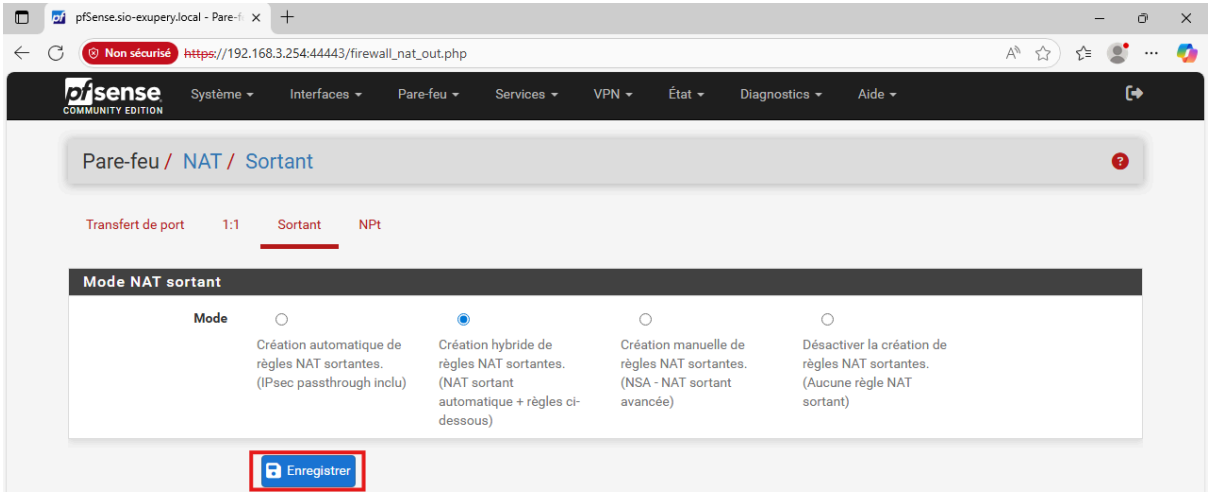

Non sécurisé
https://192.168.3.254:44443/firewall_virtual_ip_edit.php
pfsense COMMUNITY EDITION
Système
Interfaces
Pare-feu
Services
VPN
État
Diagnostics
Aide
Pare-feu / IPs virtuels / Modifier
Modifier l'IP virtuelle
Type
Alias IP
CARP
Mandataire (proxy) ARP
Autre
Interface
OPT1
Type d'adresse
Adresse unitaire
Adresse(s)
192.168.2.252
/ 24
Le masque doit être le masque de sous-réseau du réseau. Il ne spécifie pas une plage CIDR.
Mot de passe d'IP virtuelle
Entrez le mot de passe du groupe VHID.
Confirmer
Groupe VHID
102
Entrez le nom du groupe VHID qui sera partagé.
Advertising Frequency
1
Base
0
Biais
La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.
Description
CARP DMZ
Une description peut être saisie ici à des fins de référence administrative (non analysée).
Enregistrer


Non sécurisé
https://192.168.3.254:44443/firewall_virtual_ip.php
pfsense COMMUNITY EDITION
Système
Interfaces
Pare-feu
Services
VPN
État
Diagnostics
Aide
Pare-feu / IPs virtuels
Les modifications ont été appliquées avec succès.
Adresse IP virtuelle
Adresse IP virtuelle
Interface
Type
Description
Actions
192.168.1.103/24 (vhid: 100)
WAN
CARP
CARP WAN
192.168.3.252/24 (vhid: 101)
LAN
CARP
CARP LAN
192.168.2.252/24 (vhid: 102)
OPT1
CARP
CARP DMZ
Ajouter

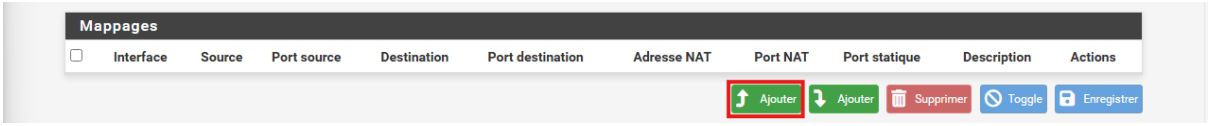


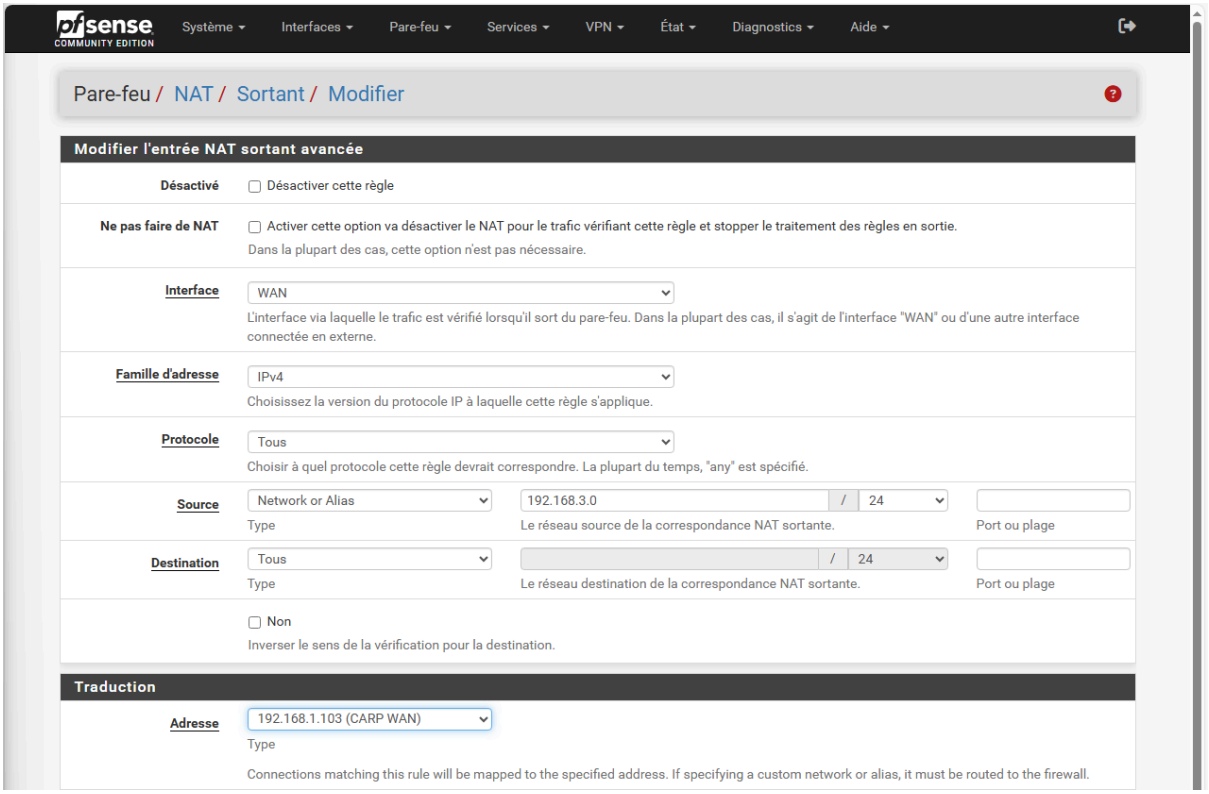



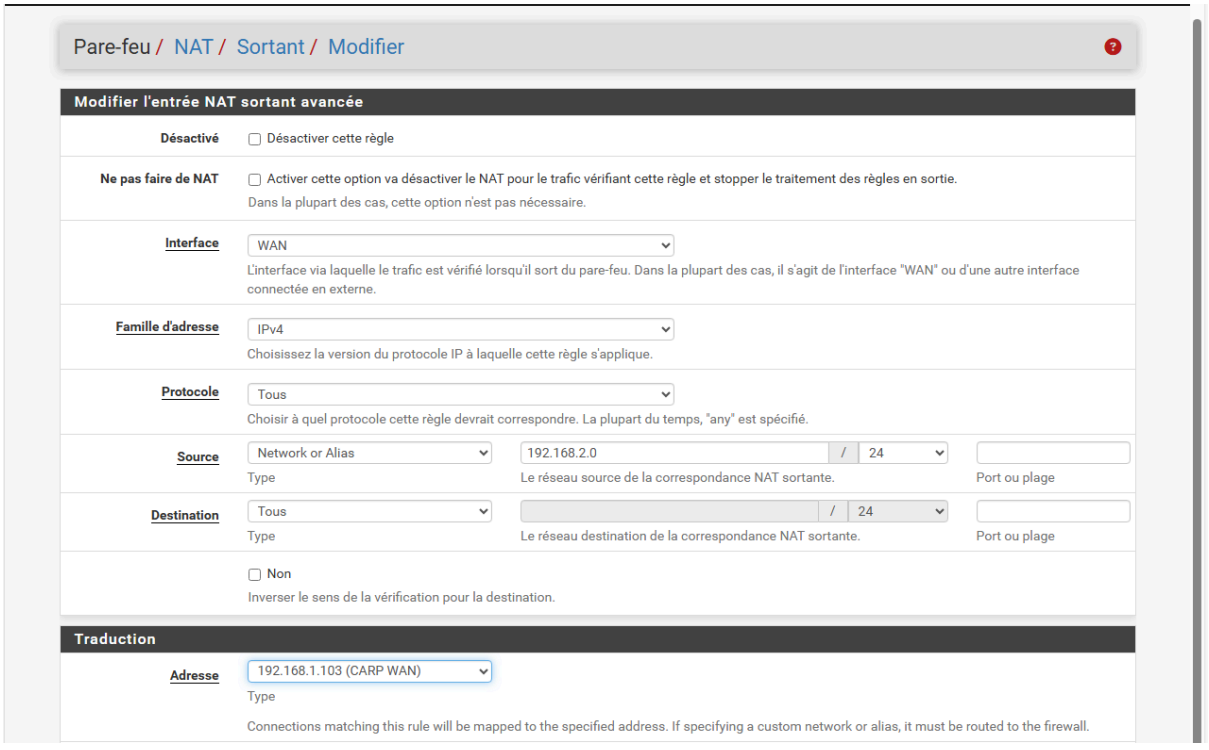

▪ Sur le pfsense Master :

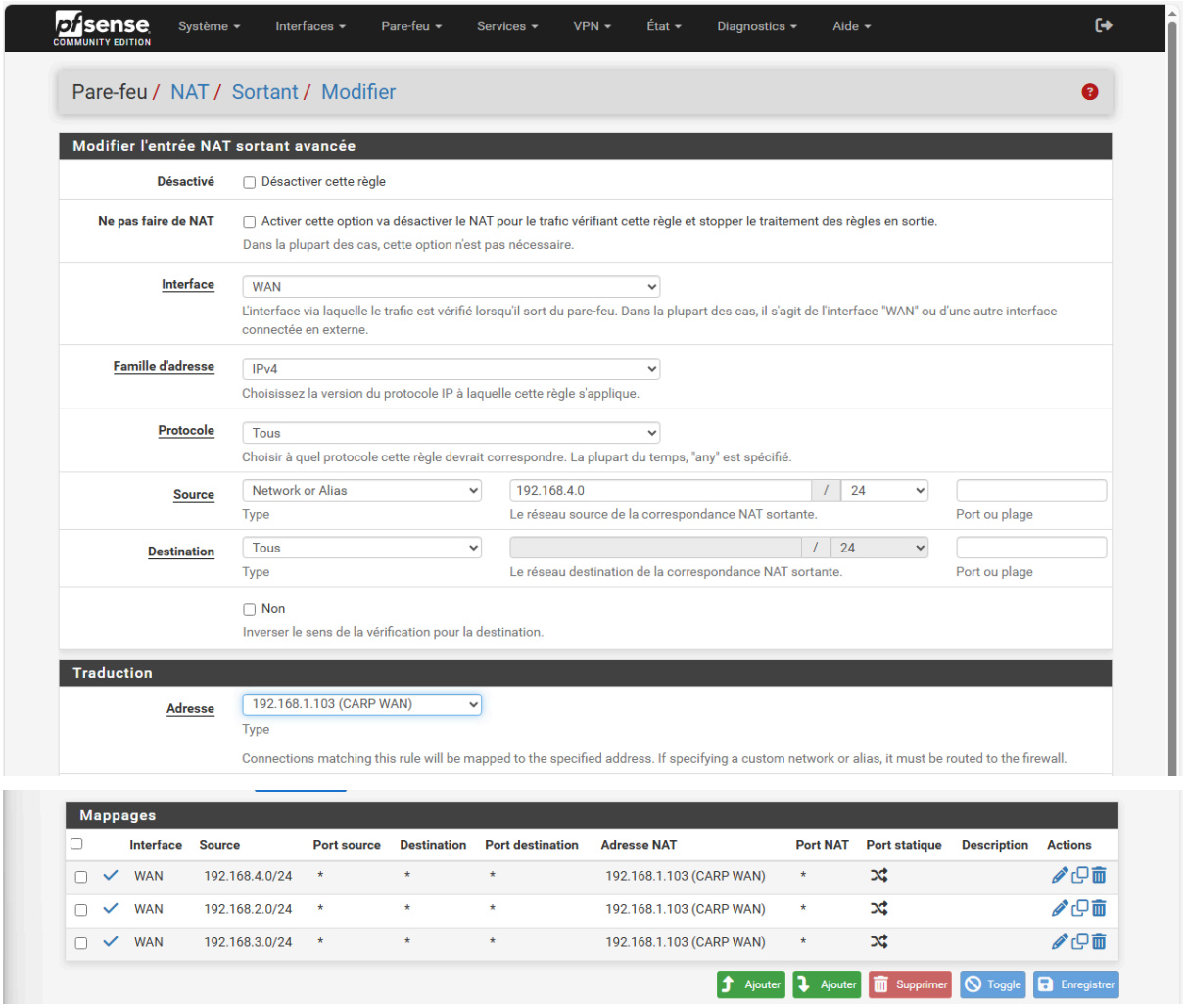



(ou Création manuelle)



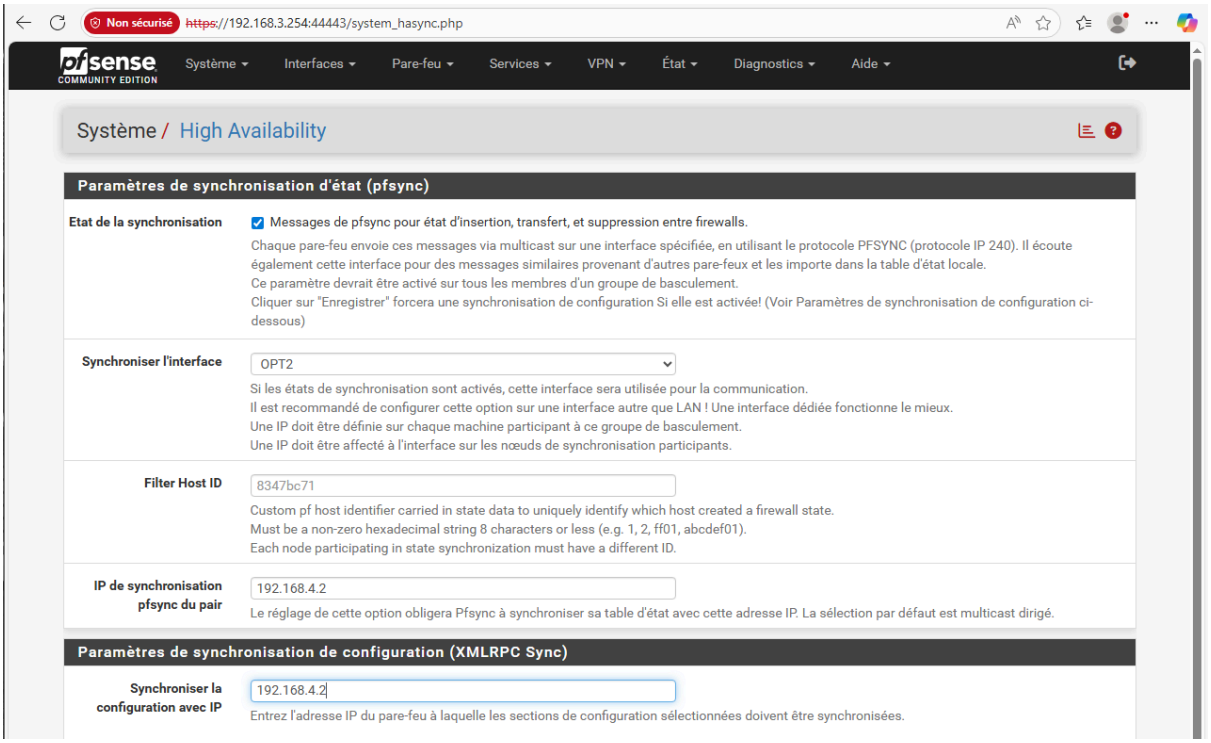

pfsense COMMUNITY EDITION
Système
Interfaces
Pare-feu
Services
VPN
État
Diagnostics
Aide
Pare-feu / NAT / Sortant / Modifier
Modifier l'entrée NAT sortant avancée
Désactivé
Désactiver cette règle
Ne pas faire de NAT
Activer cette option va désactiver le NAT pour le trafic vérifiant cette règle et stopper le traitement des règles en sortie.
Dans la plupart des cas, cette option n'est pas nécessaire.
Interface
WAN
L'interface via laquelle le trafic est vérifié lorsqu'il sort du pare-feu. Dans la plupart des cas, il s'agit de l'interface "WAN" ou d'une autre interface connectée en externe.
Famille d'adresse
IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.
Protocole
Tous
Choisir à quel protocole cette règle devrait correspondre. La plupart du temps, "any" est spécifié.
Source
Network or Alias
192.168.3.0
24
Type
Le réseau source de la correspondance NAT sortante.
Port ou plage
Destination
Tous
Type
Le réseau destination de la correspondance NAT sortante.
Port ou plage
Non
Inverser le sens de la vérification pour la destination.
Traduction
Adresse
192.168.1.103 (CARP WAN)
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

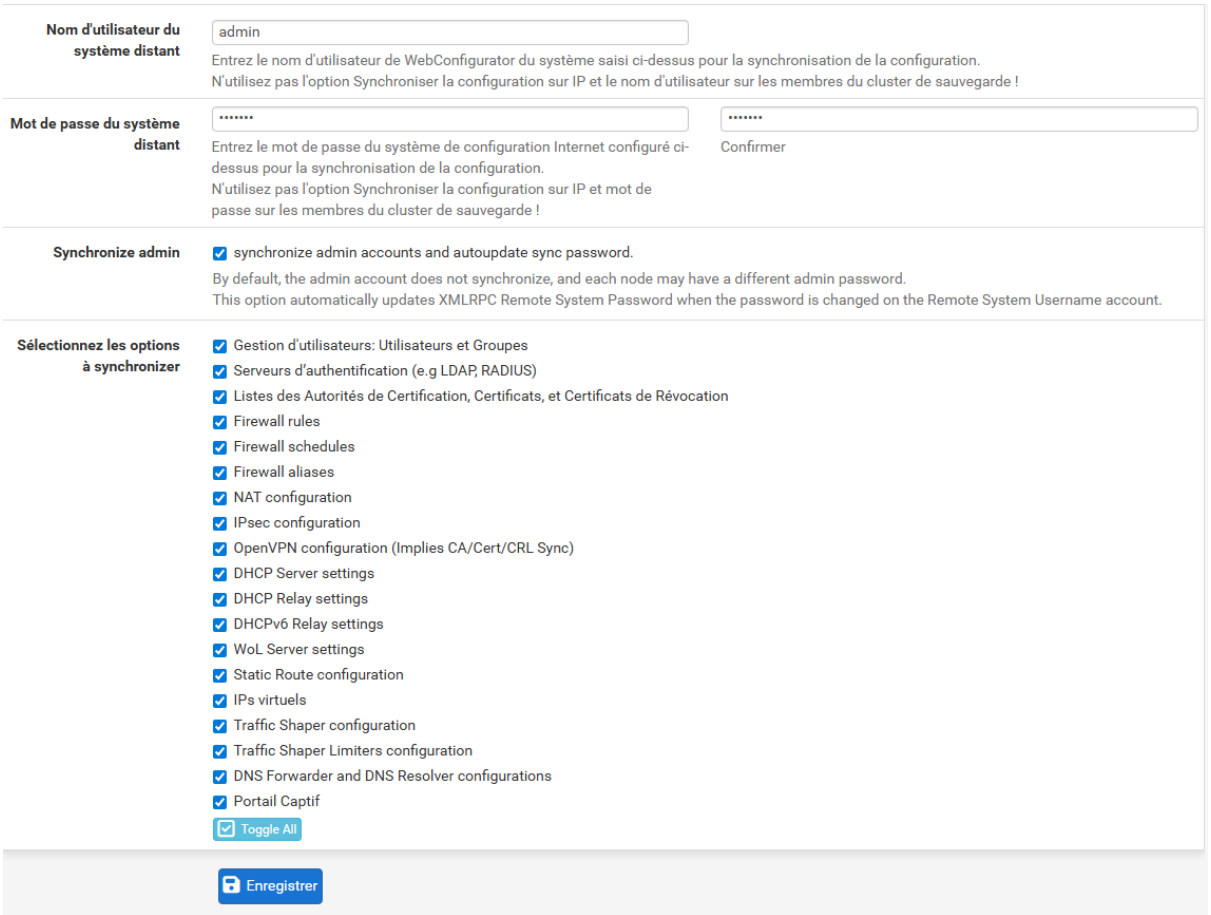

Pare-feu / NAT / Sortant / Modifier
Modifier l'entrée NAT sortant avancée
Désactivé
Désactiver cette règle
Ne pas faire de NAT
Activer cette option va désactiver le NAT pour le trafic vérifiant cette règle et stopper le traitement des règles en sortie.
Dans la plupart des cas, cette option n'est pas nécessaire.
Interface
WAN
L'interface via laquelle le trafic est vérifié lorsqu'il sort du pare-feu. Dans la plupart des cas, il s'agit de l'interface "WAN" ou d'une autre interface connectée en externe.
Famille d'adresse
IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.
Protocole
Tous
Choisir à quel protocole cette règle devrait correspondre. La plupart du temps, "any" est spécifié.
Source
Network or Alias
192.168.2.0
24
Type
Le réseau source de la correspondance NAT sortante.
Port ou plage
Destination
Tous
Type
Le réseau destination de la correspondance NAT sortante.
Port ou plage
Non
Inverser le sens de la vérification pour la destination.
Traduction
Adresse
192.168.1.103 (CARP WAN)
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.


pfsense COMMUNITY EDITION
Système
Interfaces
Pare-feu
Services
VPN
État
Diagnostics
Aide
Pare-feu / NAT / Sortant / Modifier
Modifier l'entrée NAT sortant avancée
Désactivé
Désactiver cette règle
Ne pas faire de NAT
Activer cette option va désactiver le NAT pour le trafic vérifiant cette règle et stopper le traitement des règles en sortie.
Dans la plupart des cas, cette option n'est pas nécessaire.
Interface
WAN
L'interface via laquelle le trafic est vérifié lorsqu'il sort du pare-feu. Dans la plupart des cas, il s'agit de l'interface "WAN" ou d'une autre interface connectée en externe.
Famille d'adresse
IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.
Protocole
Tous
Choisir à quel protocole cette règle devrait correspondre. La plupart du temps, "any" est spécifié.
Source
Network or Alias
192.168.4.0
24
Type
Le réseau source de la correspondance NAT sortante.
Port ou plage
Destination
Tous
24
Type
Le réseau destination de la correspondance NAT sortante.
Port ou plage
Non
Inverser le sens de la vérification pour la destination.
Traduction
Adresse
192.168.1.103 (CARP WAN)
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

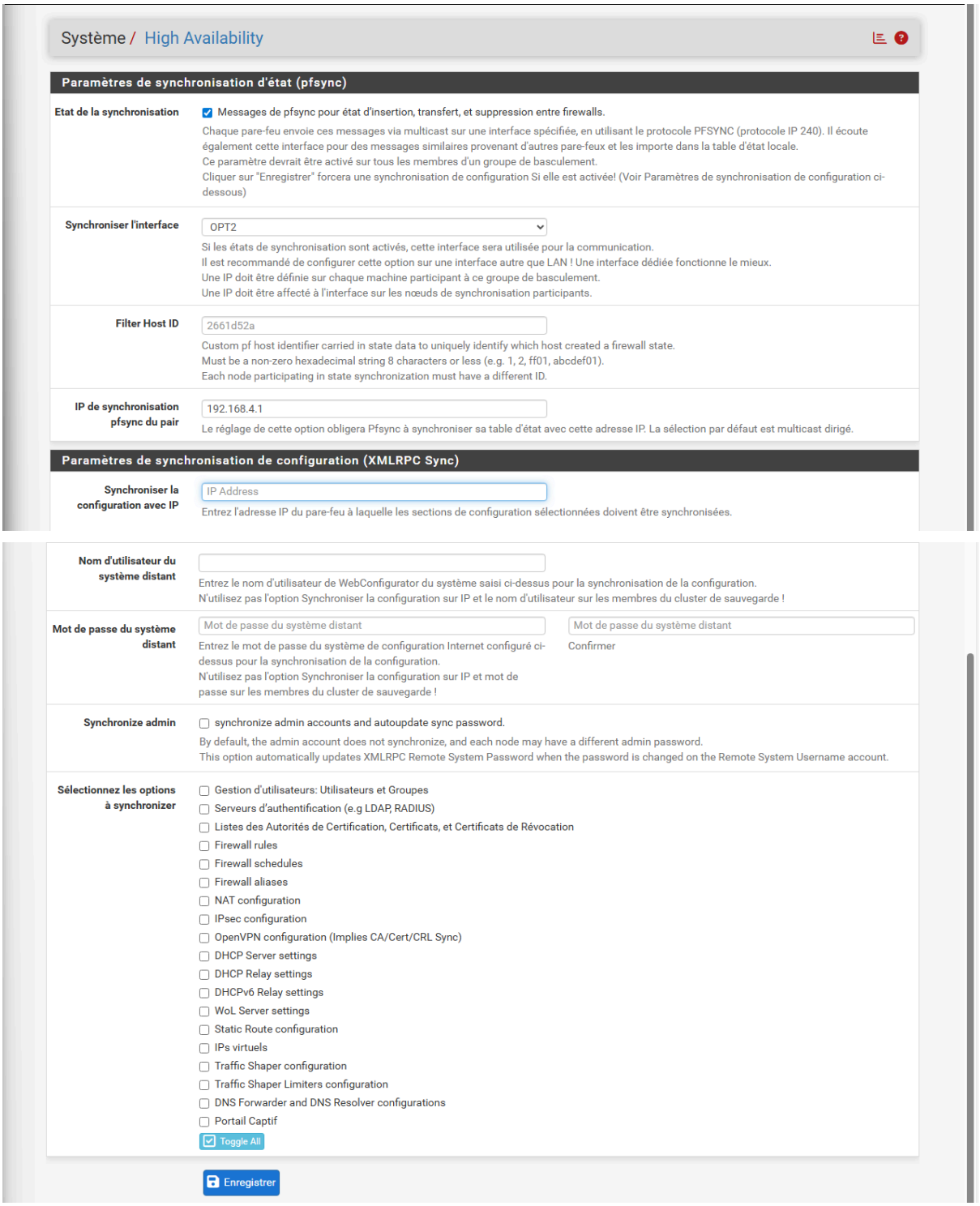

Mappages
Interface
Source
Port source
Destination
Port destination
Adresse NAT
Port NAT
Port statique
Description
Actions
WAN 192.168.4.0/24 * * * 192.168.1.103 (CARP WAN) *
WAN 192.168.2.0/24 * * * 192.168.1.103 (CARP WAN) *
WAN 192.168.3.0/24 * * * 192.168.1.103 (CARP WAN) *
Ajouter
Ajouter
Supprimer
Toggle
Enregistrer

- Nous devons le faire sur les deux PfSense
  - Nous appliquons le protocole Pfsync (pas XMLRPC)

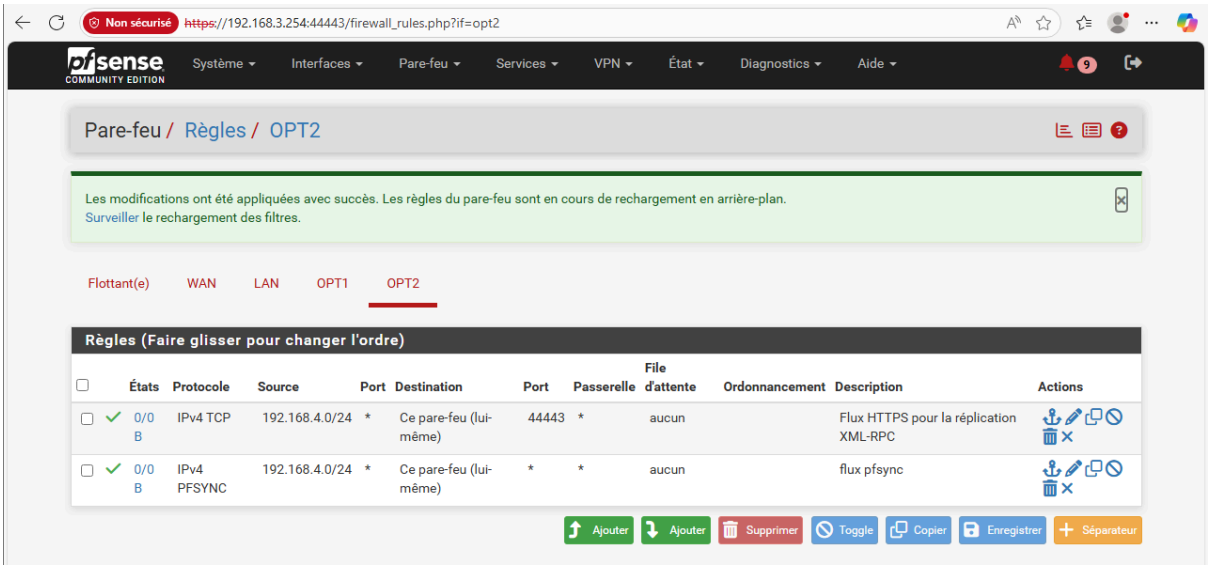


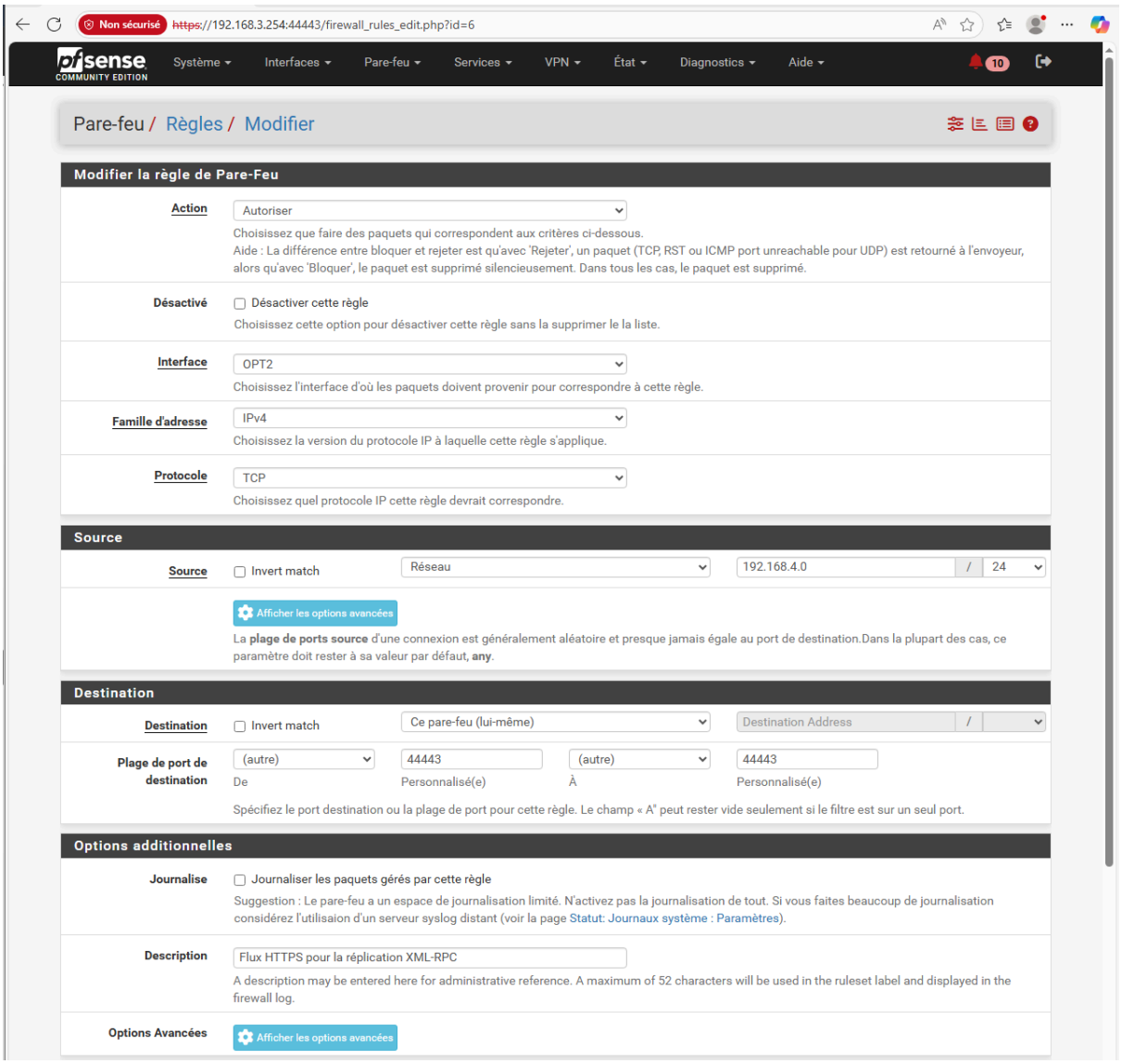



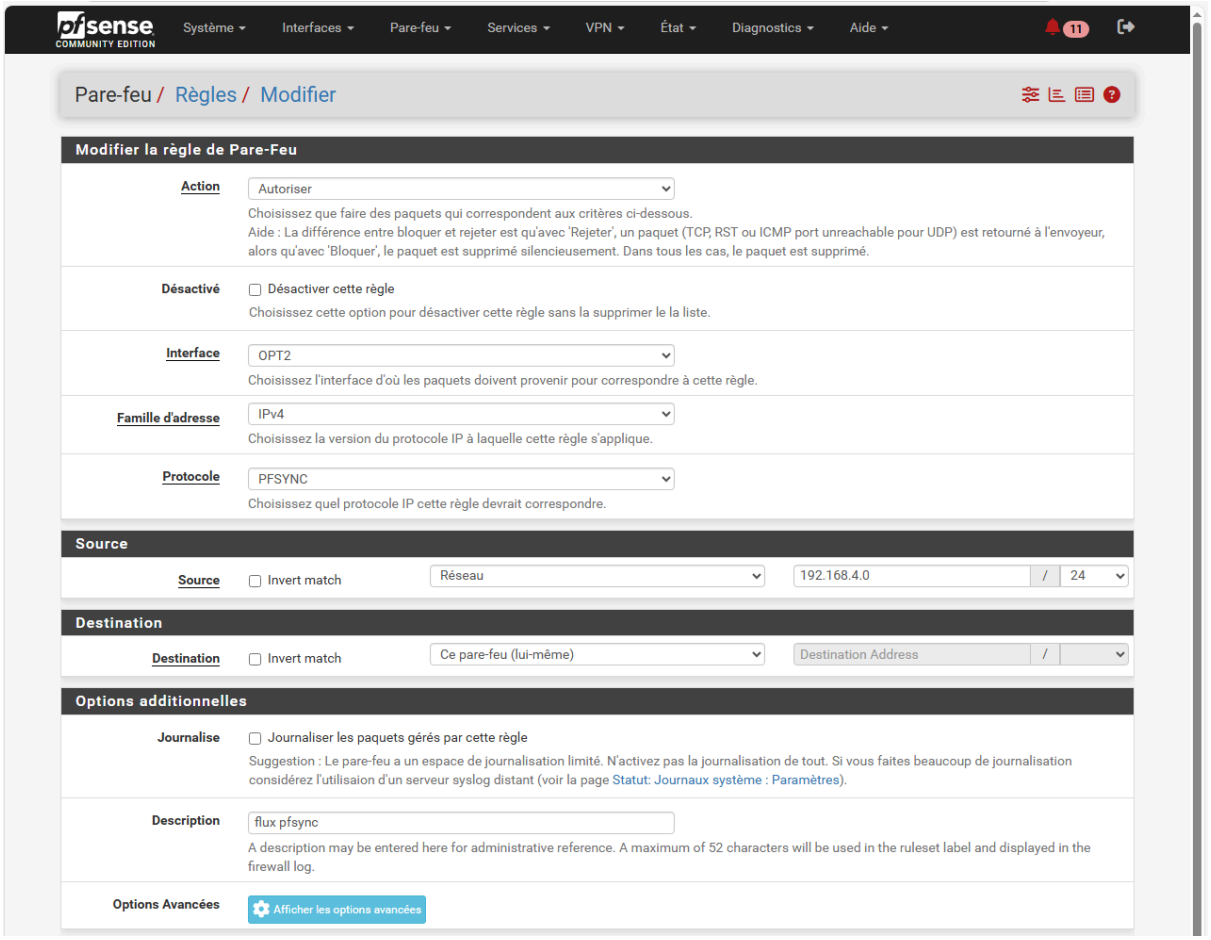
- Sur Pfsense2 :



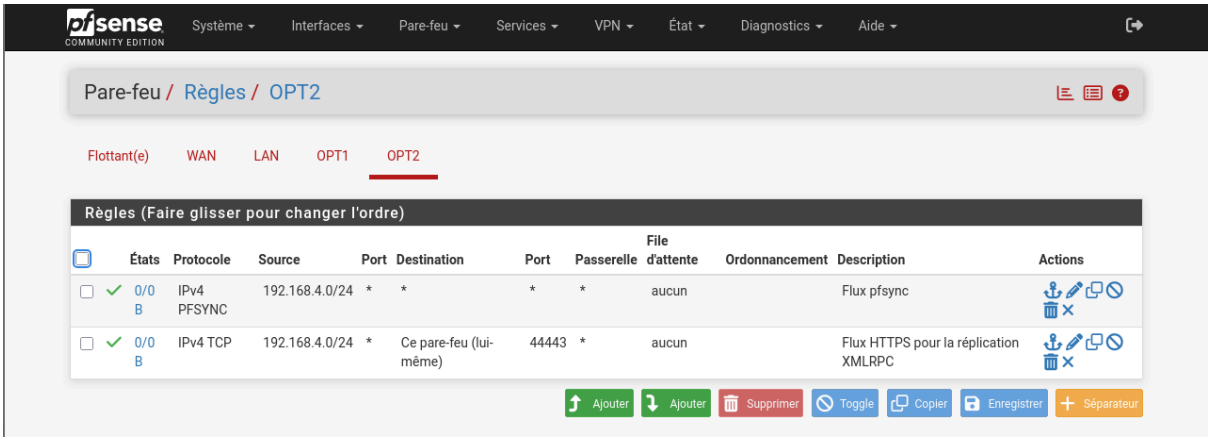
▪ Nous appliquons les règles sur le pfsense Master pour autoriser les flux pfsync et XML-RPC :

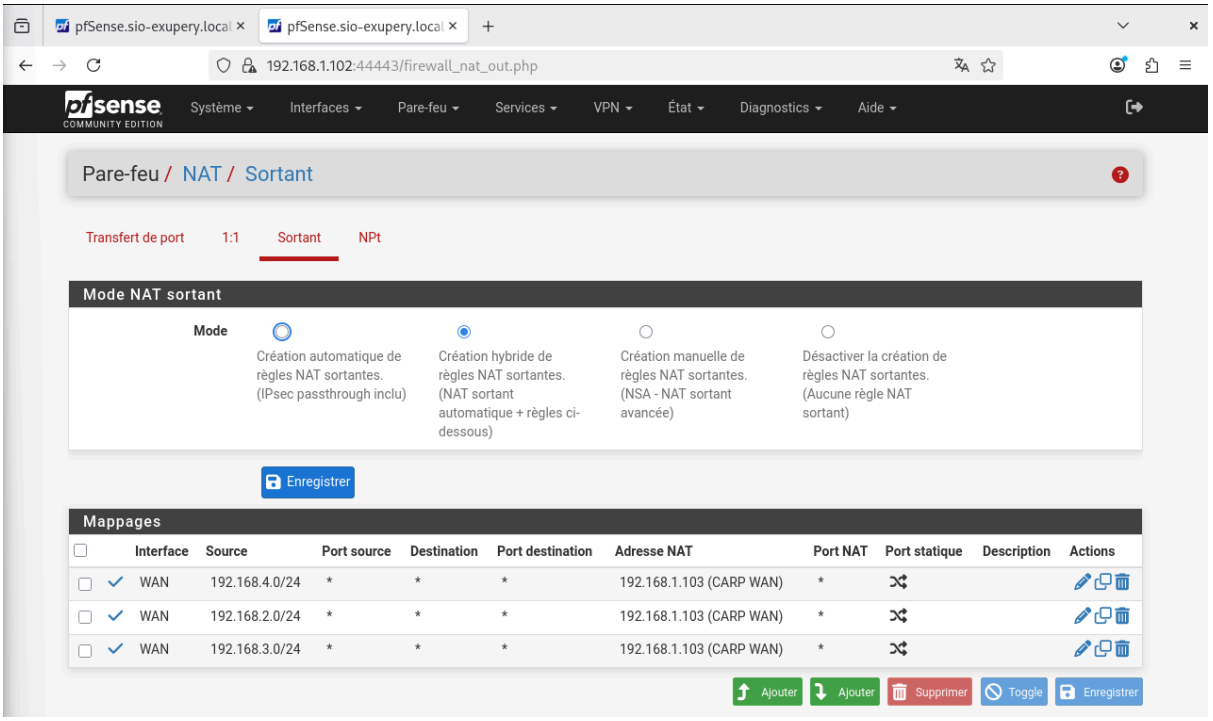


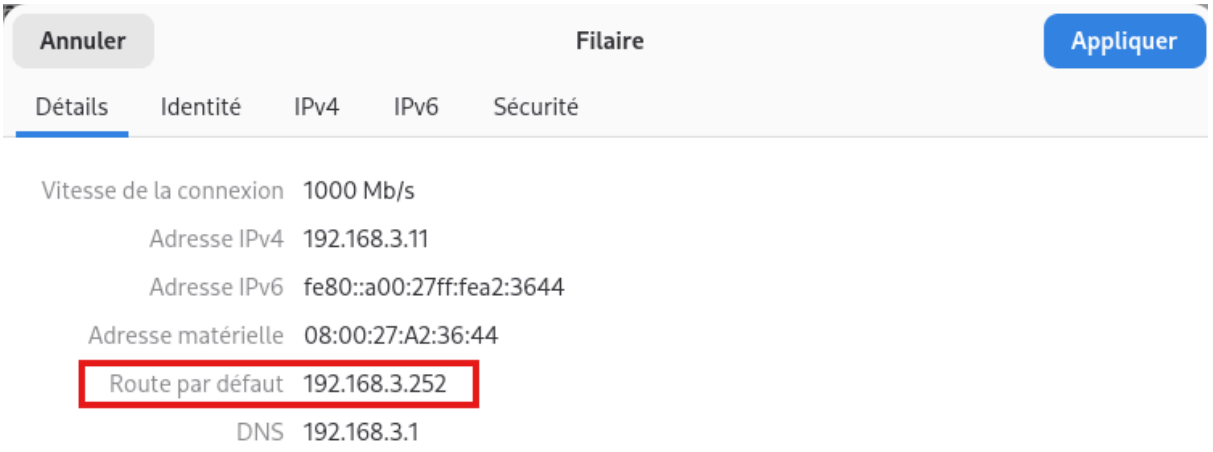



- Nous vérifions sur la pfsenseB






Test ping la machine physique :

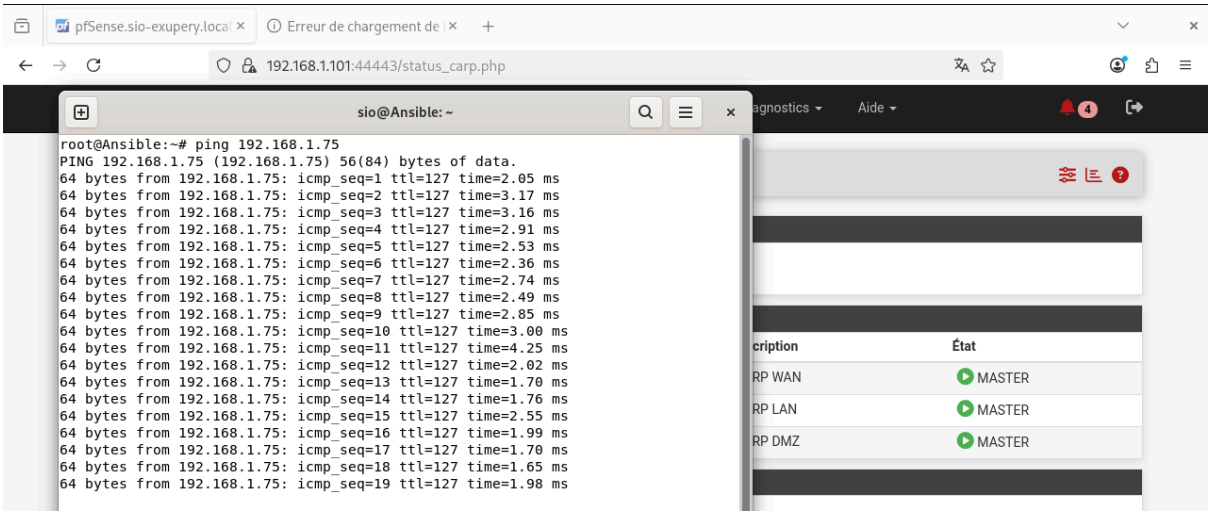



```
rtt min/avg/max/mdev = 9.904/13.410/65.281/3.482 ms, pipe 4
root@Ansible:~# ping 192.168.1.75
PING 192.168.1.75 (192.168.1.75) 56(84) bytes of data.
64 bytes from 192.168.1.75: icmp_seq=1 ttl=127 time=4.28 ms
64 bytes from 192.168.1.75: icmp_seq=2 ttl=127 time=4.78 ms
64 bytes from 192.168.1.75: icmp_seq=3 ttl=127 time=2.80 ms
64 bytes from 192.168.1.75: icmp_seq=4 ttl=127 time=2.62 ms
64 bytes from 192.168.1.75: icmp_seq=5 ttl=127 time=10.2 ms
```

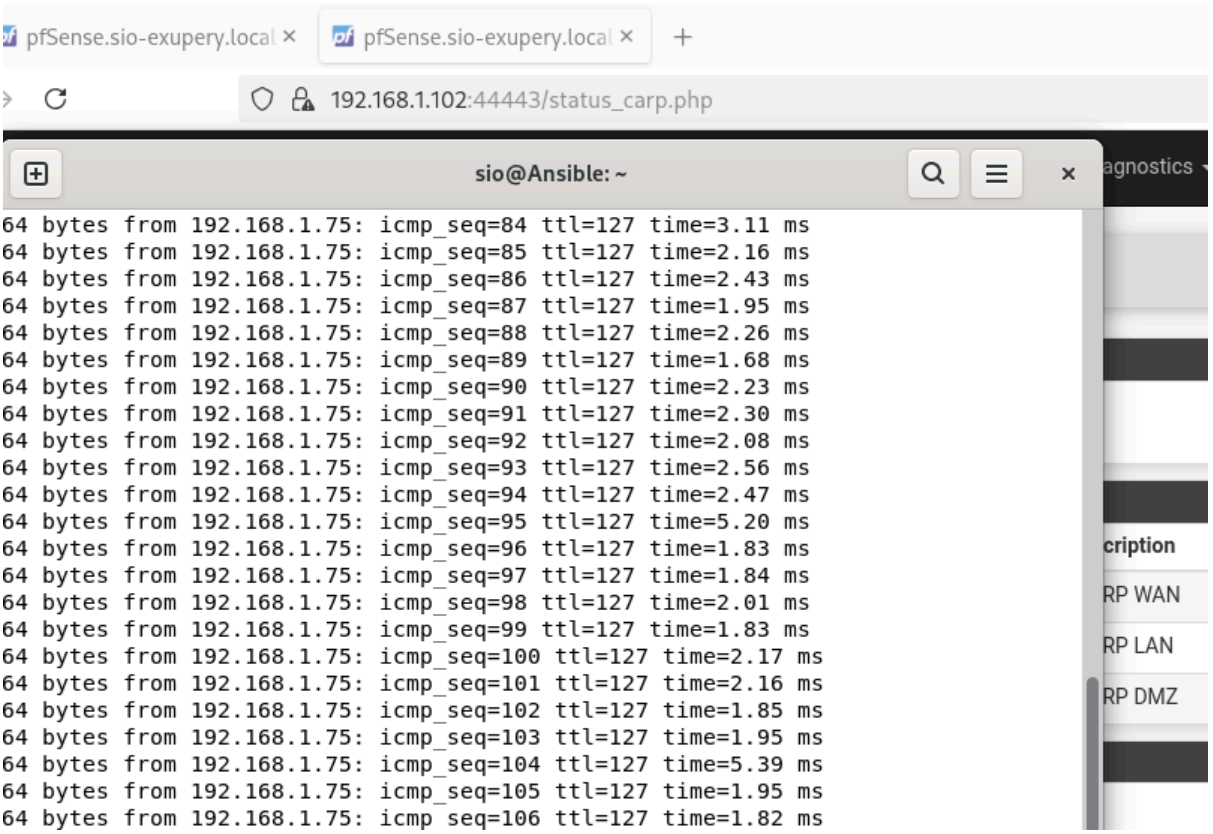
TEST Ping machine physique depuis LAN (ou ping routeur cisco ou ping 8.8.8.8) puis arrêt pfsenseA :
Ip de la machine physique à ping :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6. . . . . . . . . . . . . .: 2a02:842a:83c7:b001:7a0d:1b75:26bc:5a5b
   Adresse IPv6 temporaire . . . . . . . .: 2a02:842a:83c7:b001:202e:c3bf:2b15:371b
   Adresse IPv6 de liaison locale. . . . .: fe80::c98e:792:6a1:f08e%17
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.75
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : fe80::ce19:a8ff:fecf:70df%17
                                            192.168.1.1

Carte réseau sans fil Connexion au réseau local* 9 :
```

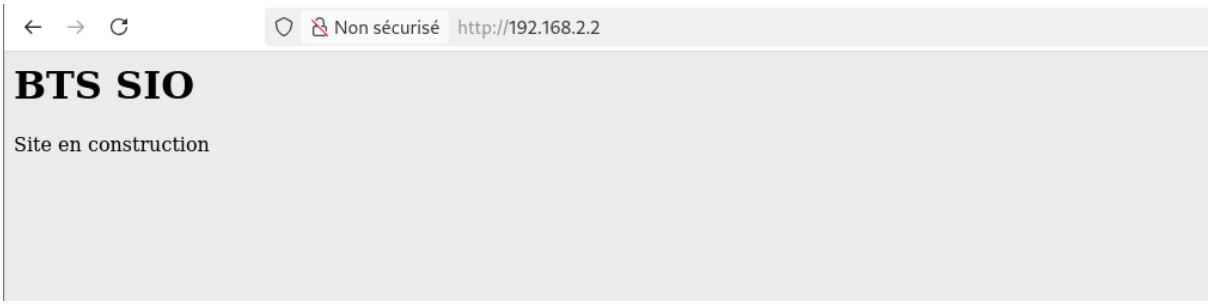
Avec pfsense A



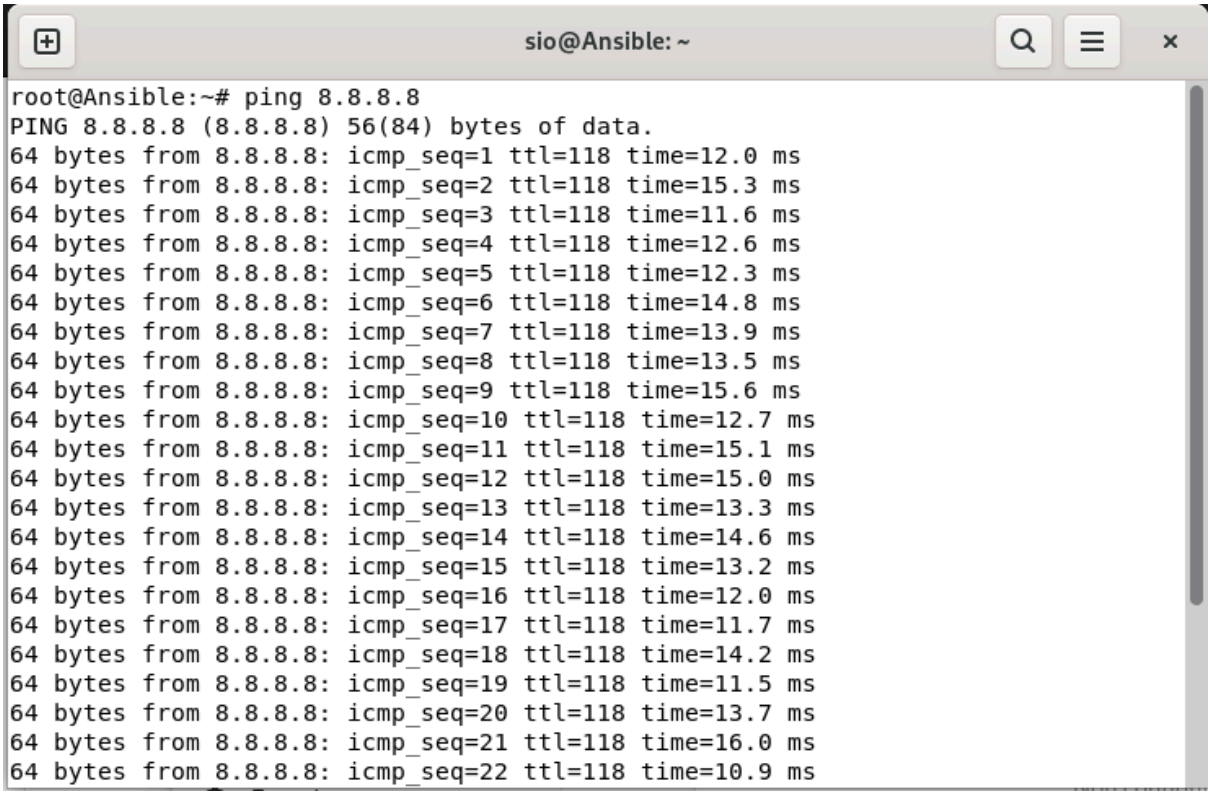

Nous arrêtons pfsenseA pour laisser place au pfsenseB




La pfsenseB prend bien le relais




Nous testons de ping 8.8.8.8


sio@Ansible: ~
root@Ansible:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=15.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=11.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=12.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=14.8 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=13.5 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=12.7 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=15.0 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=118 time=13.3 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=118 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=118 time=13.2 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=118 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=118 time=11.7 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=118 time=14.2 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=118 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=118 time=13.7 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=118 time=16.0 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=118 time=10.9 ms