Ayoub Belbachir

CARP pfsync

Cours : BLOC 1
Professeur : M. A. Ouldcheikh
Date : 17/02/2022

INTRO

nous allons configurer la haute disponibilité dans pfSense à l'aide du protocole CARP (Common Address Redundancy Protocol) et du protocole pfsync.

Ce laboratoire suppose que vous avez déjà installé et configuré les paramètres de pare-feu de base tels que les attributions d'adresses IP, à la fois WAN et LAN.

Le but du Failover, c'est donc de faire en sorte que si mon pfSense-01 venait à tomber, le 02 prendrait le relais,

Pour cela, il existe le protocole **CARP**, pour *Common Address Redundancy Protocol*, littéralement *Protocole de redondance d'adresses communes*. Le titre est assez clair, ce protocole permet à plusieurs hôtes d'utiliser une même IP pour effectuer de la redondance.

Ensuite, nous utiliserons les protocoles **pfSync** et **XML-RPC**, qui permettent respectivement de synchroniser l'état des connexions en cours entre deux hôtes Pfsense et pour le second de répliquer la configuration.

PRÉ-REQUIS

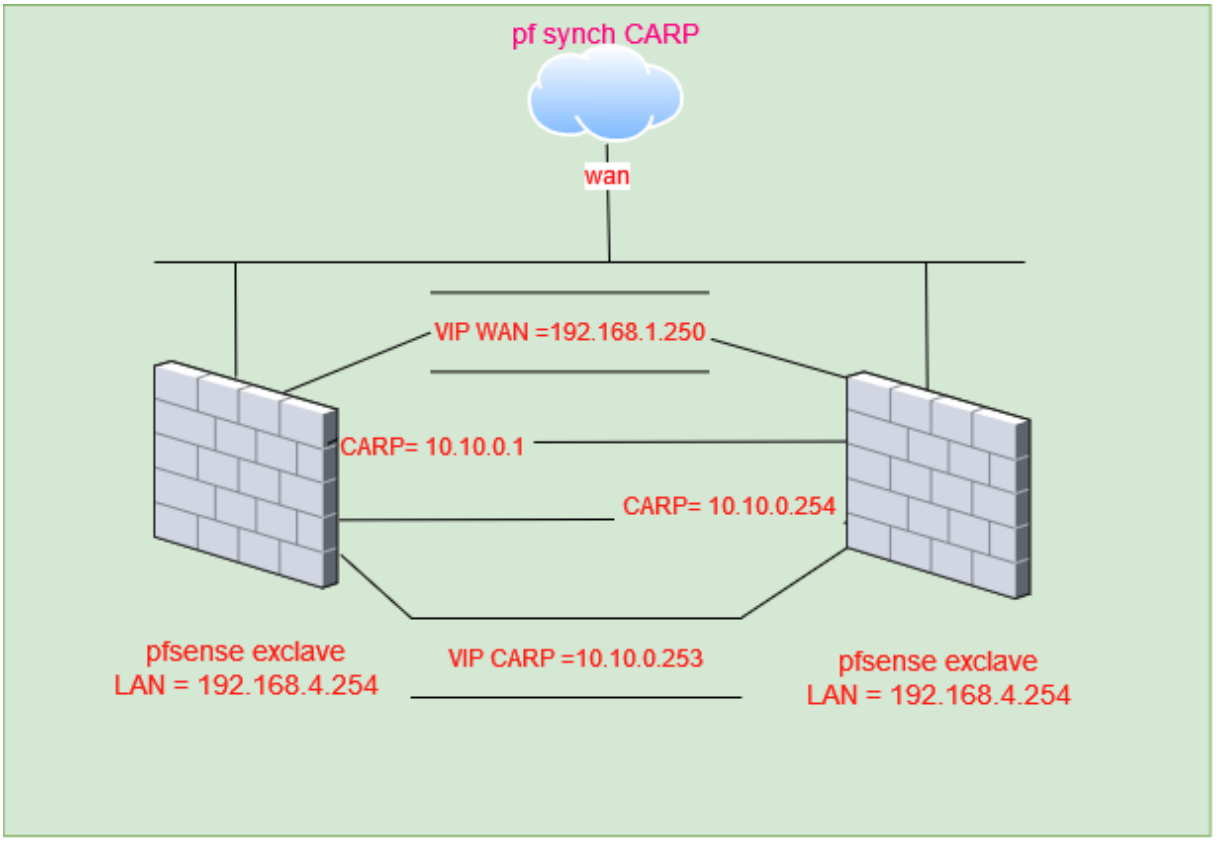
- Oracle VirtualBox
- 2 VM PFSENSE >
  - Allocation mémoire RAM: 1go
  - Stockage : 20 go
  - Iso : PFSENSE
  - 1er Carte Réseau 'ACCÈS PAR PONT' :
  - 2nd Carte Réseau « Interne » 'INET' :
  - 3eme Carte Réseau « Interne » 'CARP' :

- 1 VM windows >
  - Allocation mémoire RAM : 6gb
  - Stockage : 50 go
  - Iso : WINDOWS 10
  - 1er Carte Réseau « Interne » 'INET' :

Ayoub Belbachir

CARP pfsync

SCHÉMA-LOGIQE



- **pfSense-Maitre** :
  - IP WAN en : 192.168.1.75/24
  - Une IP LAN en : 192.168.4.1/24
  - Une IP pour la carte CARP en 10.10.0.1/30
  - Une IP virtuelle pour la carte CARP en : 10.10.0.253/30
  - Une IP virtuelle pour le WAN en : 192.168.4.250/24

- **pfSense-Exclave** :
  - Une IP WAN en : 192.168.1.76/24
  - Une IP LAN en : 192.168.4.254/24
  - Une IP pour la carte CARP en 10.10.0.254/30
  - Une IP virtuelle pour la carte CARP en : 10.10.0.253/30
  - Une IP virtuelle pour le WAN en : 192.168.4.250/24

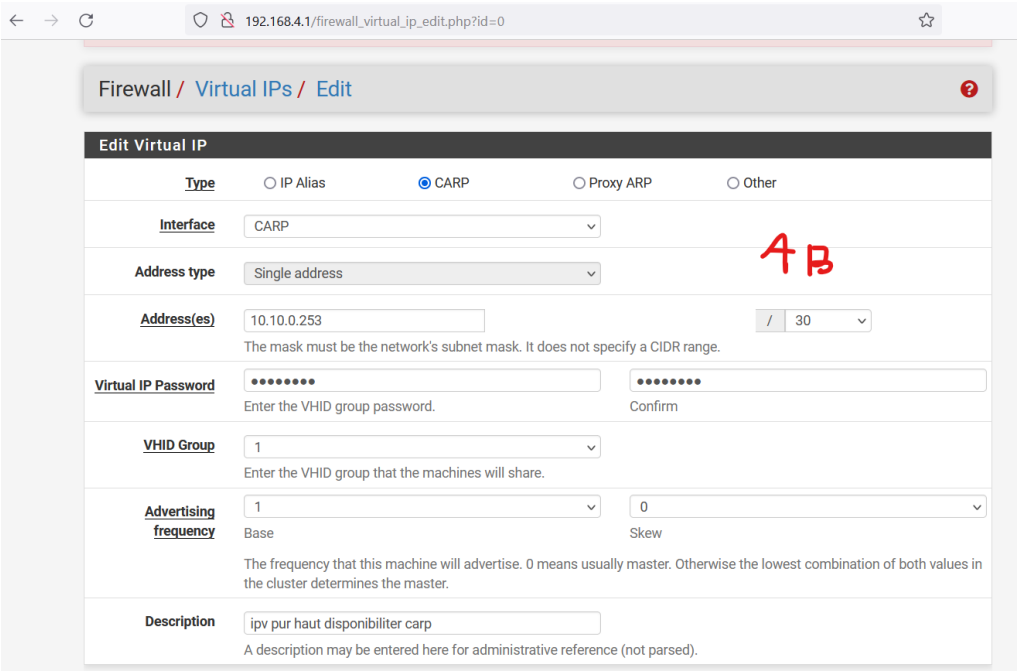
Ayoub Belbachir

CARP pfsync

TUTORIEL

Mise en place des interfaces virtuelles

La première étape est donc de créer nos deux interfaces virtuelles, sur chacun de nos hôtes. Pour cela on se rend sur Firewall puis Virtual IPs puis Add :

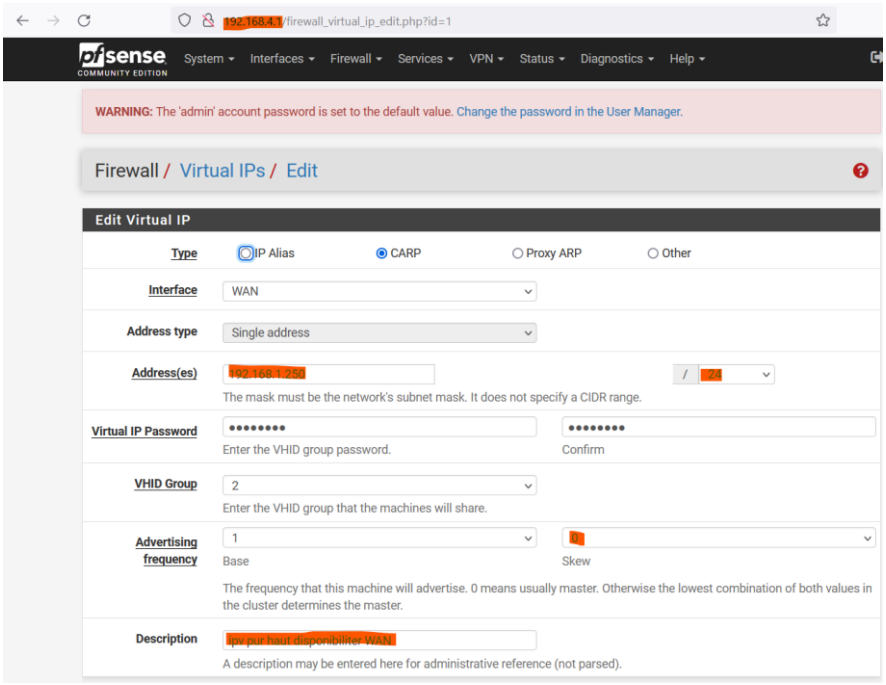


Ici on choisit donc le type CARP, car nous avons aussi la possibilité d'utiliser l'IP Alias ou encore le Proxy ARP, mais ce n'est pas le cas ici. On choisit ensuite notre interface, CARP pour commencer, puis on renseigne donc l'adresse IP virtuel ainsi que le masque de sous réseau. Nous renseignons un mot de passe qui sera utilisé pour le groupe VHID. On vient ensuite justement renseigner l'ID de ce fameux groupe, car un même Pfsense peut faire partie de plusieurs clusters, pour l'interface Carp nous renseignons de l'ID 1 et pour l'interface wan nous renseignons de l'ID 2. Et enfin, nous laissons la valeur Base à 1 (qui correspond au nombre de secondes avant qu'un hôte soit considéré comme down) et pour la valeur Skew, nous la laissons à valeur à 0. Cette valeur devra être modifier pour le Pfsense exclave à savoir Skew=100, ici nous sommes sur notre Pfsense-Maitre qui sera le master donc nous laissons cette valeur (0).

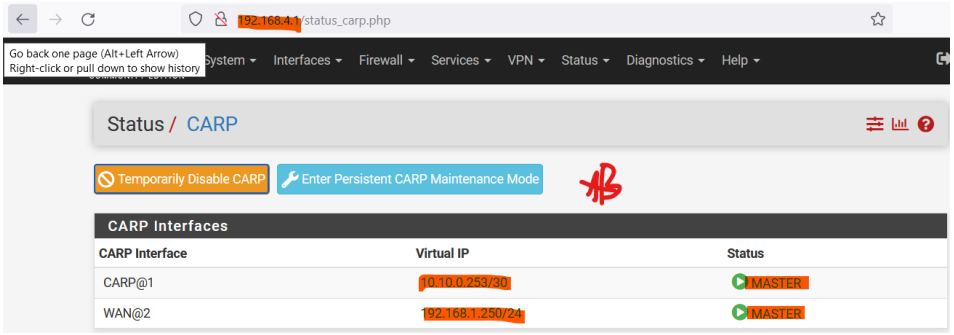
Ayoub Belbachir

CARP pfsync

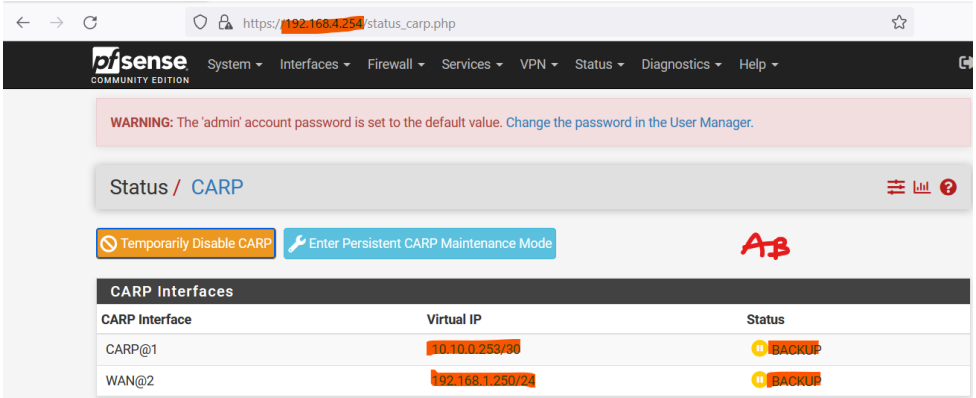
Configuration pour l'interface WAN



Rendez-vous dans l'onglet Status puis CARP (failover) on devrait avoir ceci, après avoir réalisé les manipulations indiquées sur le Pfsense :



Et depuis le Pfsense exclave :

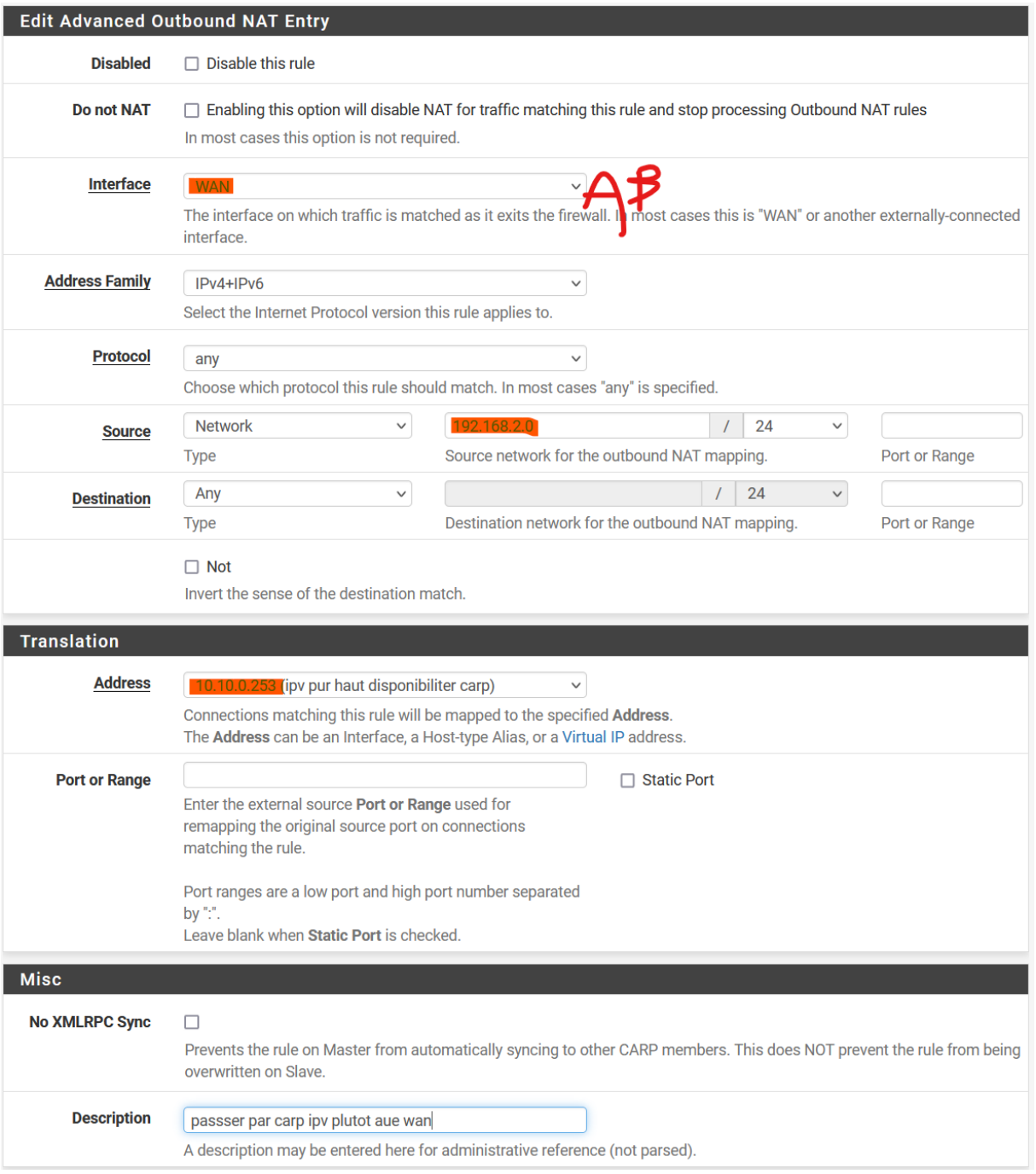


Ayoub Belbachir

CARP pfsync

Ensuite nous devons indiquer à Pfsense d'utiliser l'IP Virtuelle plutôt que d'utiliser son IP CARP/WAN classique. Pour cela, nous nous se rendons dans Firewall puis NAT.

On choisit l'option Hybrid Outbound NAT plutôt qu'Automatic Outbound NAT, de cette manière nous allons pouvoir créer une règle qui sera prise en compte en cliquant sur Add juste en dessous de Mappings :



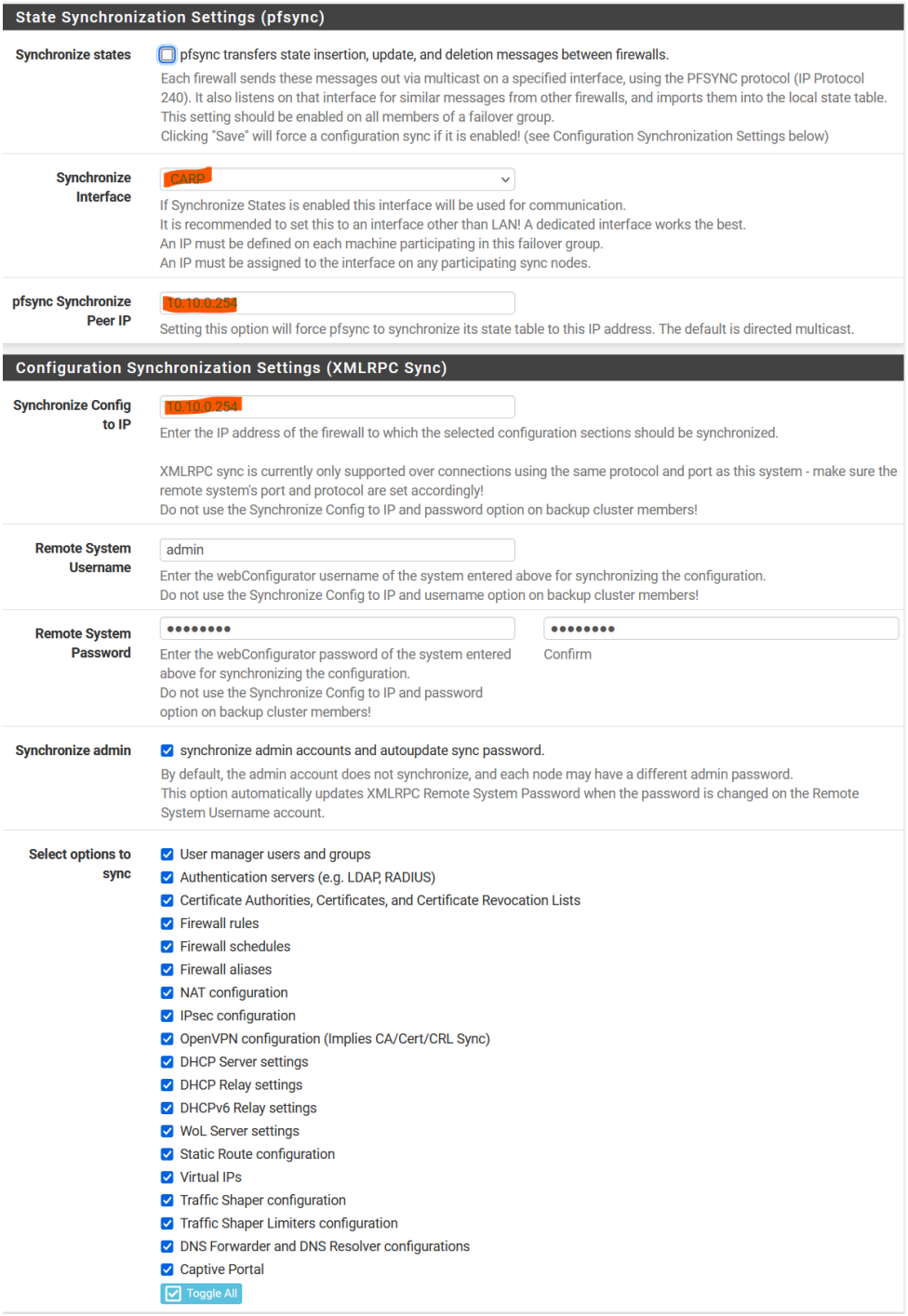
Ayoub Belbachir

CARP pfsync

Mise en place de la High-Availability

Depuis le Pfsense maitre Rendez-vous dans System, puis High Avail.Sync :

Renseignez l'adresse IP de l'interface CARP du Pfsense exclave



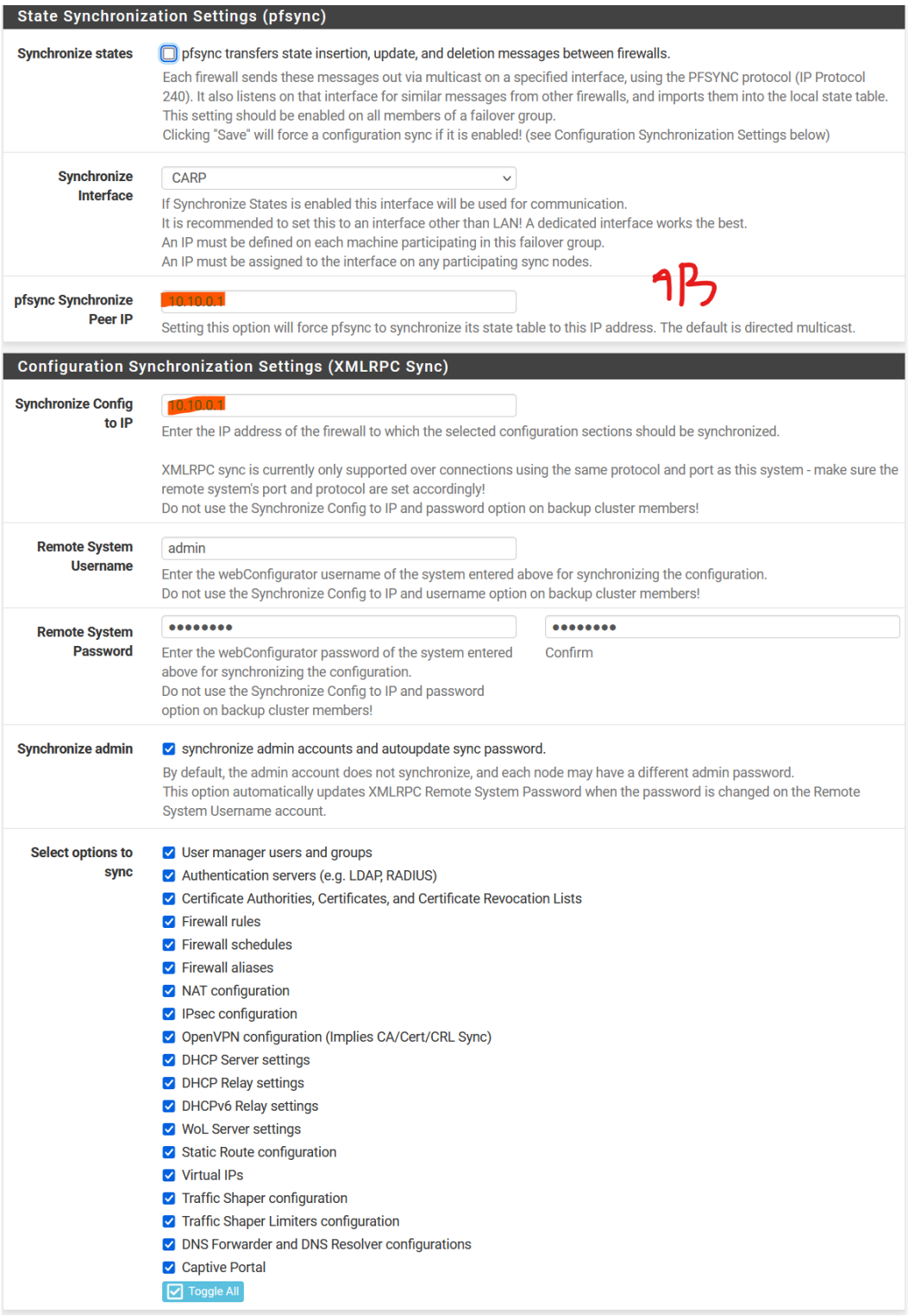
Nous voulons que la synchronisation se face des 2 sens.

Ayoub Belbachir

CARP pfsync

Depuis le Pfsense exclave Rendez-vous dans System, puis High Avail.Sync :

Renseignez l'adresse IP de l'interface CARP du Pfsense Maitre

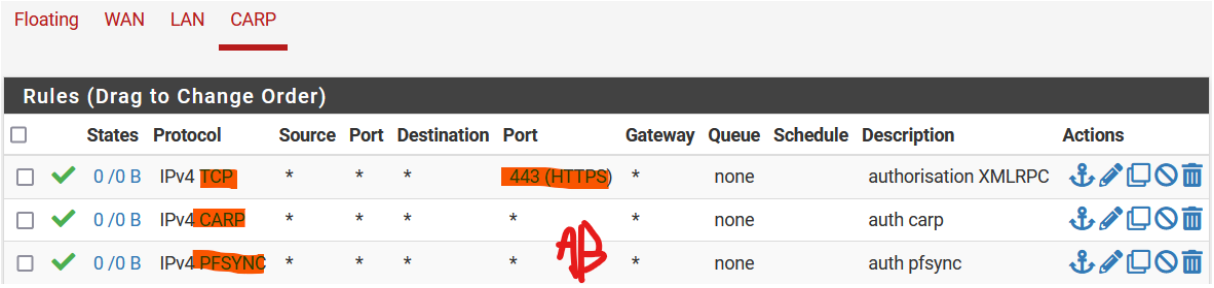


Ayoub Belbachir

CARP pfsync

Les règles de pare-feu

Par défaut les interfaces sur Pfsense bloquent tout le trafic. nous devons nous rendre dans l'onglet Firewall puis Rules et enfin CARP et copiés les règles suivantes sur les 2 Pfsense :



Ces règles permettent d'autoriser le trafique des protocoles CARP PFSYNC et XMLRPC en relation avec notre synchronisation, le Protocol XMLRPC se trouve sur dans le port HTTPS (443)

Ayoub Belbachir

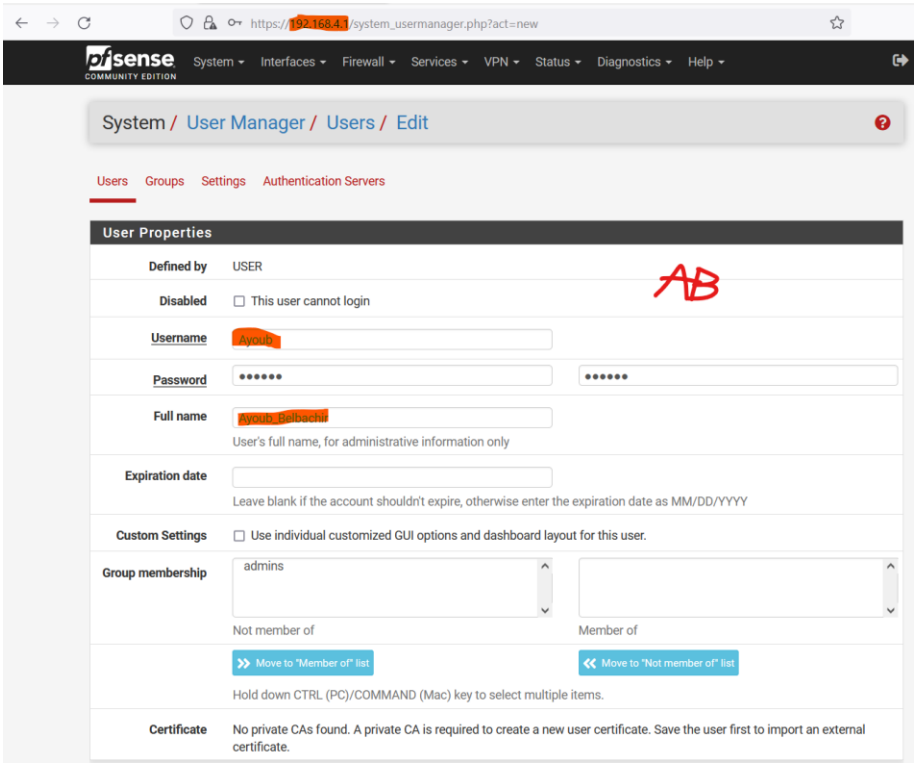
CARP pfsync

Test de la haute disponibilité

C Nous allons simplement crée un nouvel utilisateur au sein de notre Pfsense maitre et observer qu'il se réplique bien sur le Pfsense exclave.

Rendez-vous dans l'onglet System puis User Manager :

Crée un nouvel utilisateur



Depuis le Pfsense exclave rendez-vous dans l'onglet System puis User Manager on peut observer que l'utilisateur a bien été dupliqué :