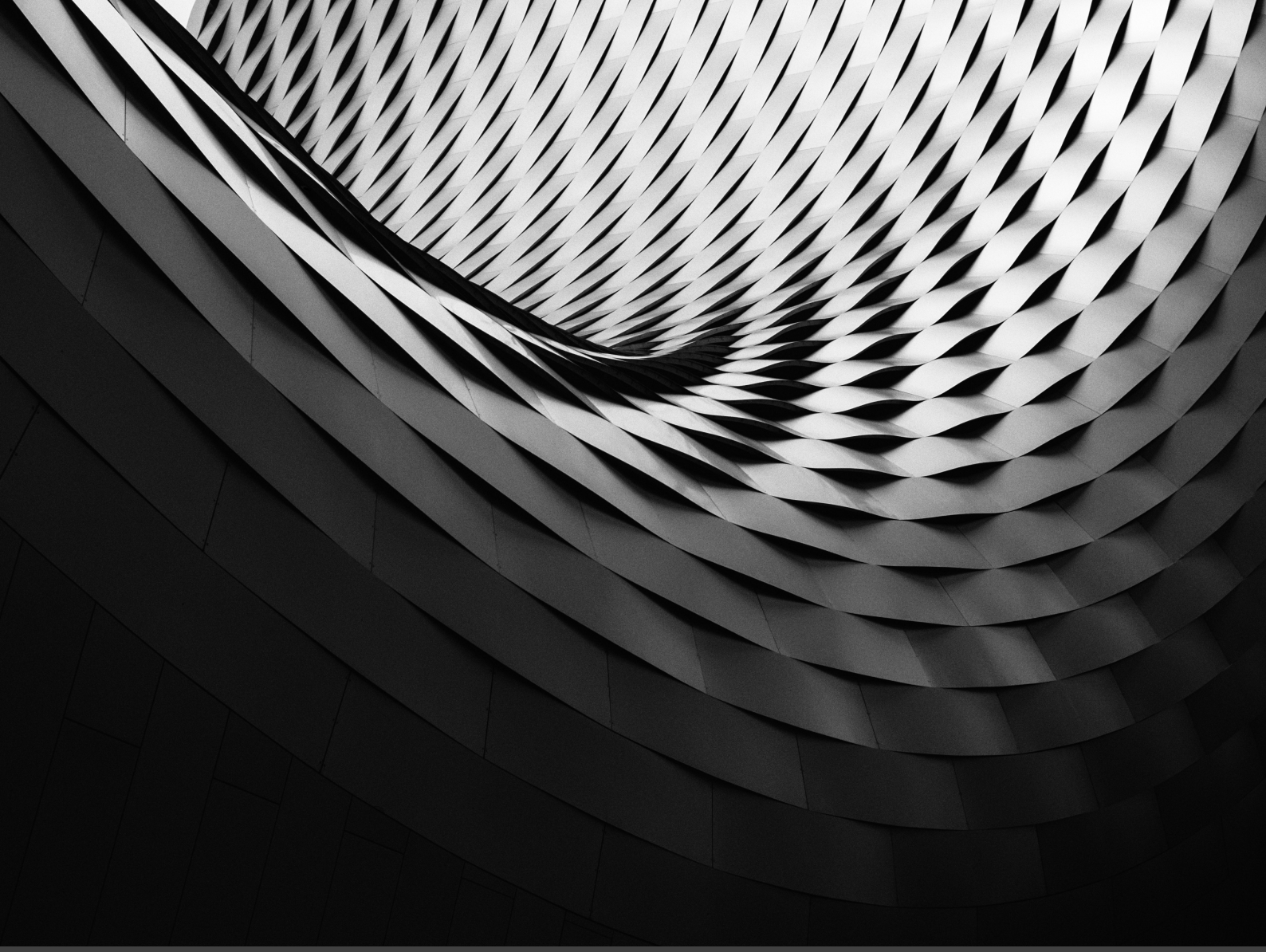


YNOV CAMPUS - RM-IT

MISE EN PLACE D'UN CLUSTER DE FIREWALL PFSENSE

OLIER CLÉMENT

2018-2019

MICKAËL RIGONNAUX

Sommaire

Documentation de la mise en place d'un Firewall PFsense en HA

Firewall PFSense en HA

Introduction

Cette documentation a pour but de présenter la mise en place d'un cluster firewall PFSense installé dans le campus Ynov d'Aix-en-Provence. Cette opération fait suite à la demande d'installation de firewall.

Les différents acteurs sont :

- Le campus Ynov d'Aix-en-Provence, école privée accueillant à peu près 600 étudiants représentée par Mr Battistoni Eric. (https://www.ynov-aix.fr/)
- La société RM-IT, société de consulting et de prestation en informatique représentée par Mr Rigonnaux Mickael et Mr Olier Clément. (https://www.rm-it.fr)

Demandes

La demande était la suivante, mettre en place un second firewall sur l'infrastructure existante afin d'avoir une tolérance de panne de cet outil indispensable sur le réseau. La demande est donc l'installation d'un nouveau firewall PFSense et sa configuration.

Plus précisément les demande du campus Ynov Aix sont les suivantes :

- Maintien de sessions en cas de panne
- Pas de coupure en cas de panne
- Bon niveau de sécurité

Cette demande inclus donc la mise en place de plusieurs protocoles :

- CARP (Common Address Redundancy Protocol) : ce dernier permet à plusieurs hôtes d'un même réseau de partager une même adresse IP, c'est-à-dire une IP virtuelle. Il est très souvent utilisé pour faire de la répartition de charge ou de la tolérance de panne. Il est une alternative libre à HSRP et VRRP.

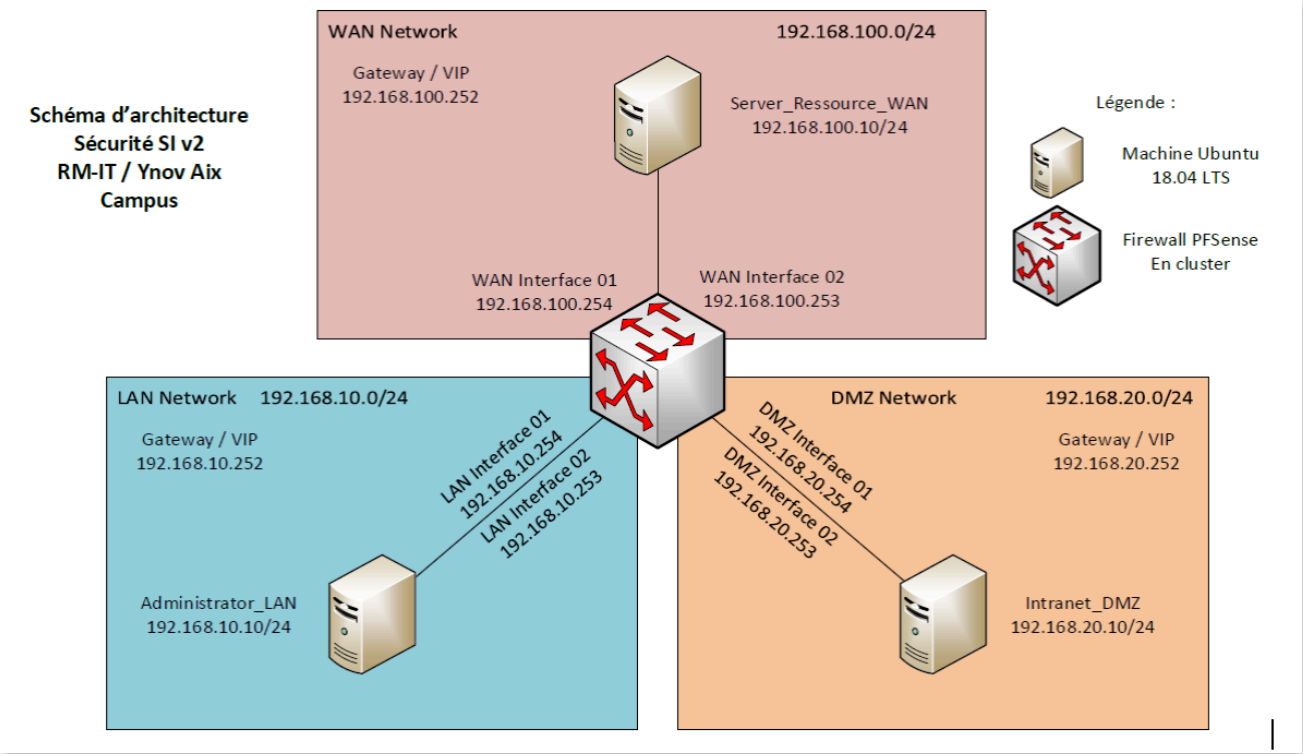
- XMLRPC (XML Remote Procedure Call) : ce dernier permet l'échange dynamique des configurations entre le PFSense maître et son esclave.
- PFSync : pfsync permet lui d'assurer la haute disponibilité d'un système en diffusants les états des connexions, c'est-à-dire des tests de vies entre les deux pares-feux.

Réalisation

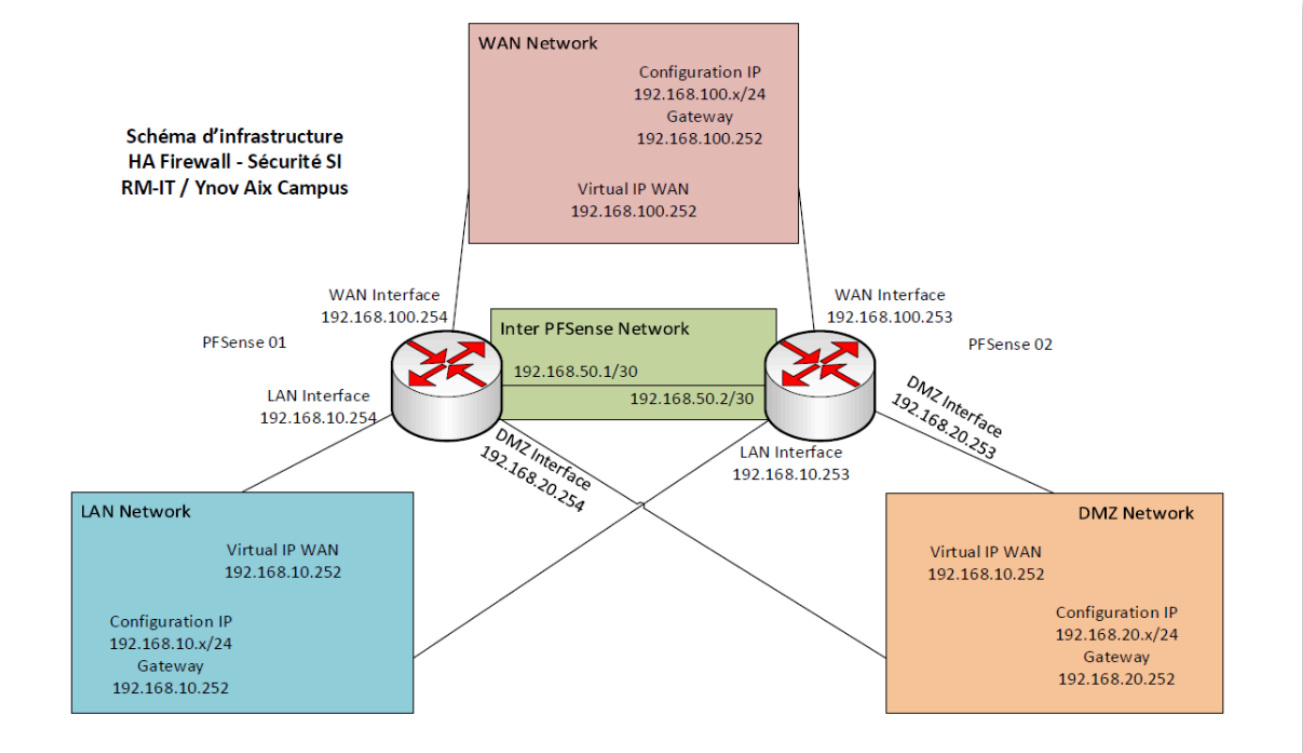
La présente infrastructure est basée sur de la virtualisation avec VMWare Workstation 15, l'ensemble des réseaux sont configurés comme des réseaux privés.

Schéma Réseau

Général



Détaillé



Sur ce second schéma nous avons une version plus détaillée du cluster de firewall PFSense et nous voyons également le nouveau réseau dédié entre les 2 pare-feu. Ce réseau est créé pour séparer les protocoles nécessaires à la mise en place de la haute disponibilité des autres réseaux. Il est aussi possible d'observer les deux firewalls distincts le PFSense 01 (maître) et le PFSense 02 (esclave).

Eléments du réseau

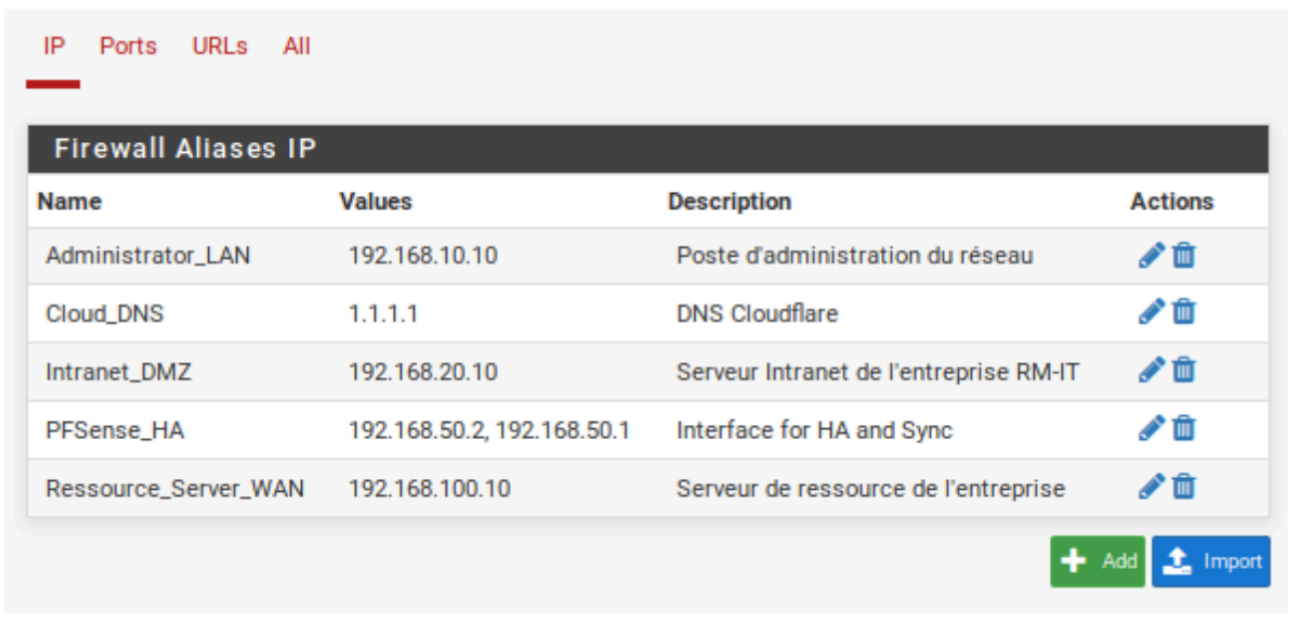
Nom	Réseau	IP	OS
Administration_LAN	LAN	192.168.10.10/24	Ubuntu 18.04 LTS
Intranet_DMZ	DMZ	192.168.20.10/24	Ubuntu 18.04 LTS
Serveur_Ressource	WAN	192.168.100.10/24	Ubuntu 18.04 LTS
PFSense 01 (Maître)	Interface 01 LAN Interface 02 WAN Interface 03 DMZ Interface 04 InterPFSense	192.168.10.254/24 192.168.100.254/24 192.168.20.254/24 192.168.50.1/30	PFSense 2.4.4
PFsense 02 (Slave)	Interface 01 LAN Interface 02 WAN Interface 03 DMZ Interface 04 InterPFSense	192.168.10.253/24 192.168.100.253/24 192.168.20.253/24 192.168.50.2/30	PFSense 2.4.4
PFSense 01 & 02 (VIP)	Interface LAN Interface WAN Interface DMZ	192.168.10.252/24 192.168.100.252/24 192.168.20.252/24	----------

Plans d'adressages

Voici les plans d'adressage des différents réseaux :

Nom	Adresse Réseau	Masque	Passerelle	DNS
WAN (simulé)	192.168.100.0	255.255.255.0	192.168.100.252	1.1.1.1
LAN	192.168.10.0	255.255.255.0	192.168.10.252	1.1.1.1
DMZ	192.168.20.0	255.255.255.0	192.168.20.252	1.1.1.1
InterPFSense	192.168.50.0	255.255.255.252	----------	----------

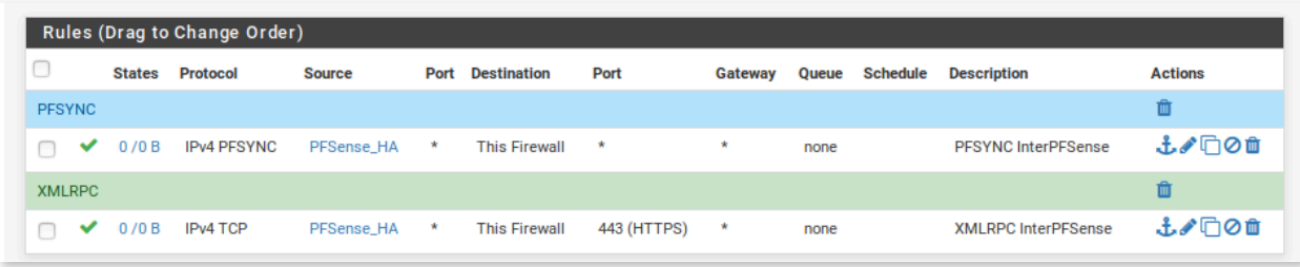
Alias



Pour la mise en place de ce second firewall un Alias de plus a été ajouté. Il correspond aux 2 IPs du réseaux InterPFSense.

Règles de Firewall

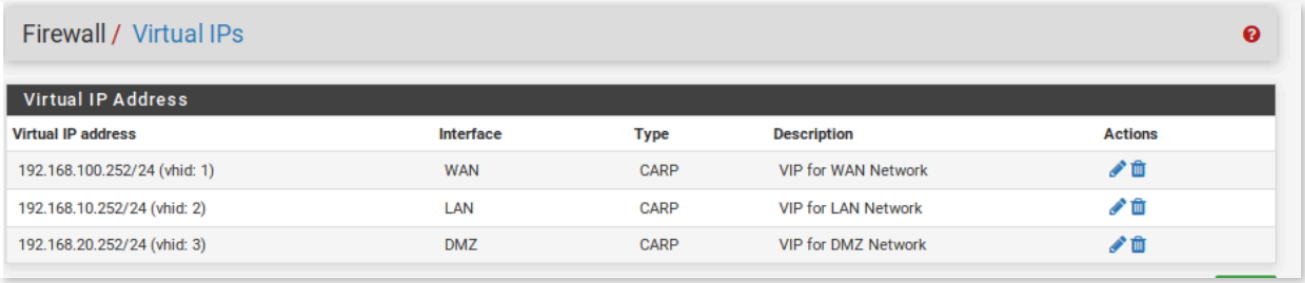
Afin de réponse favorablement aux demandes du campus Ynov Aix les règles suivantes ont été ajoutées pour le réseau InterPFSense :



La première règle permet les échanges entre les deux firewalls avec le protocole PFSYNC.
La seconde permet au protocole XMLPRC d'échanger des données entre les deux PFSense.

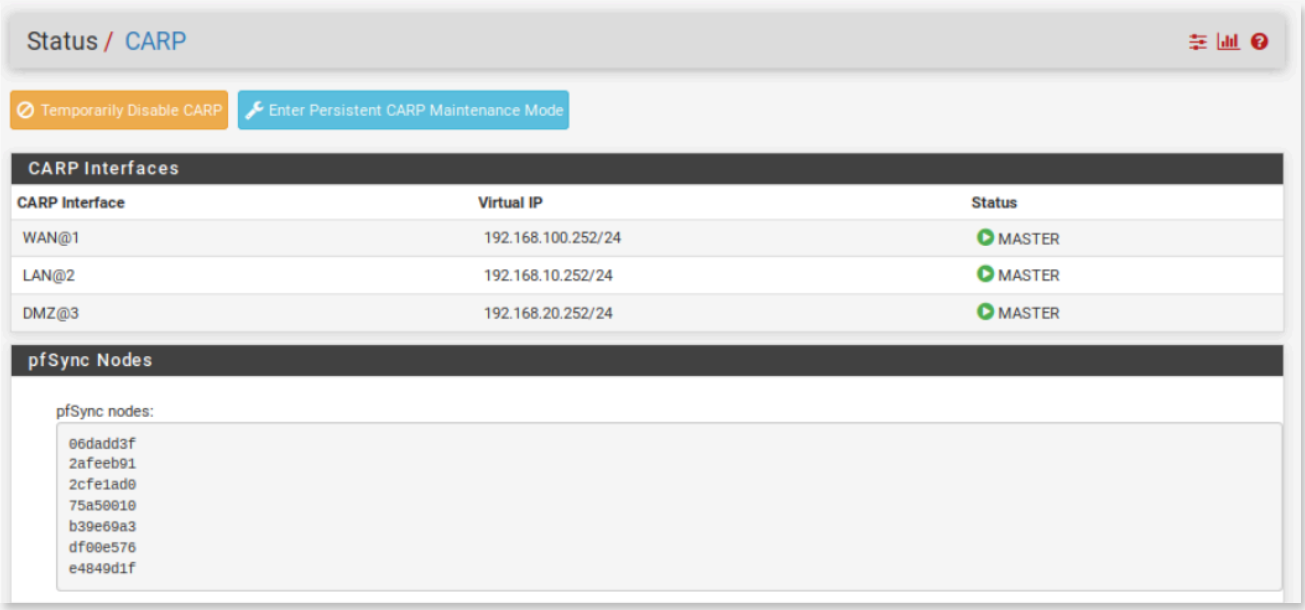
Protocole CARP

Comme vu plus haut, le protocole CARP est utilisé pour créer les IP virtuelles. Voici les IPs créées sur chacun des Firewall :

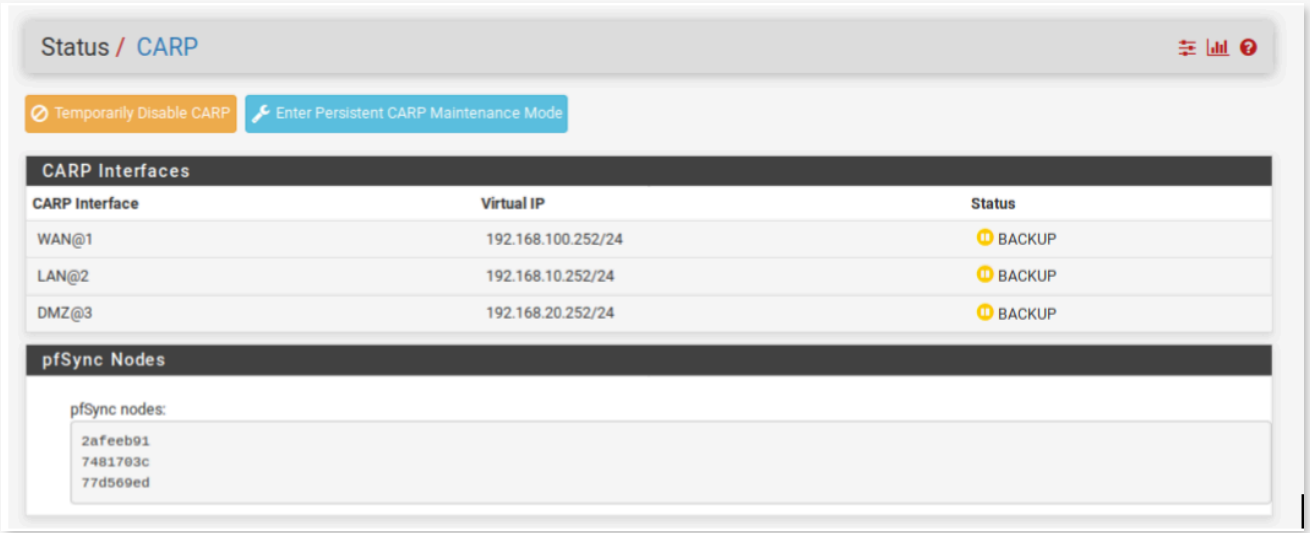


Il fonctionne également en mode master/slave. Le PFSense 01 est le master et le PFSense 02 le slav. Le PFSense 02 basculera en mode maître si le PFSense 01 rencontre un problème. Il est aussi à noter qu'avec ce protocole les passerelles de chaque réseau doivent être les IP virtuelles sinon la tolérance de panne ne fonctionnera pas. L'état de chaque firewall est vérifiable via le menu dédié :

PFSense 01



PFSense 02



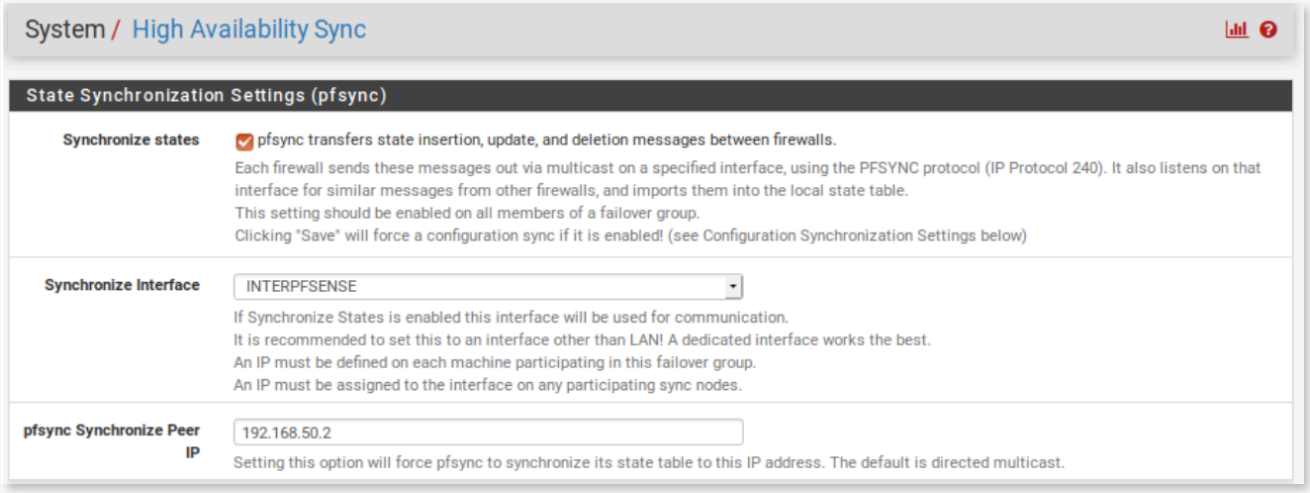
Pour vérifier le bon fonctionnement de ce processus nous avons également réalisé une capture réseau pour ce protocole sur le réseau. Il y a bien des échanges entre les réseaux, cependant ce protocole est toujours vu comme du VRRP par Wireshark.

Protocole PFsync

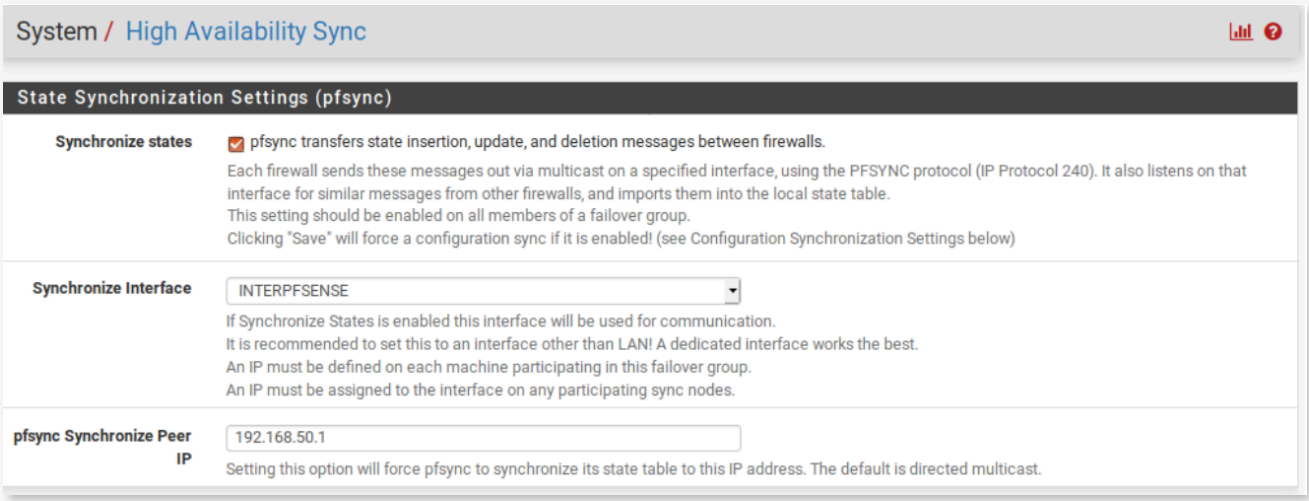
La configuration du protocole PFSync se fait aussi sur les deux firewalls dans l'onglet dédié. Deux informations sont demandées :

- Les interfaces à utiliser
- L'IP distante

Pour le PFSense 01 :



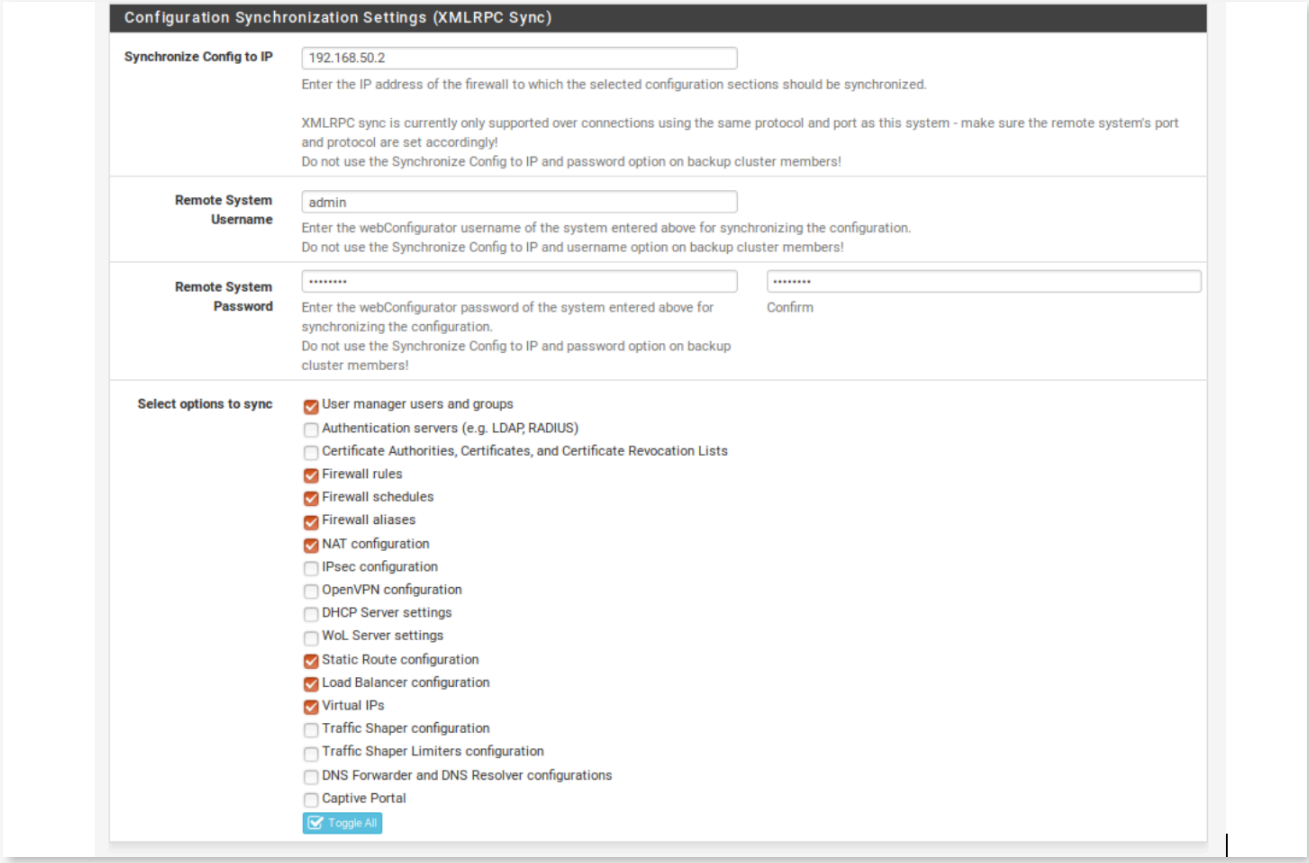
Pour le PFSense 02 :



Afin d'observer le fonctionnement et la fiabilité du protocole nous avons analysés les logs du firewall et nous avons bien remarqué la présence de paquets PFSync dans ces dernières.

Protocole XMLRPC

Pour finir le protocole XMLRPC lui permet la synchronisation des différentes configurations entre le maître et l'esclave. Il se configure lui seulement sur le PFSense 01 de la manière suivante :

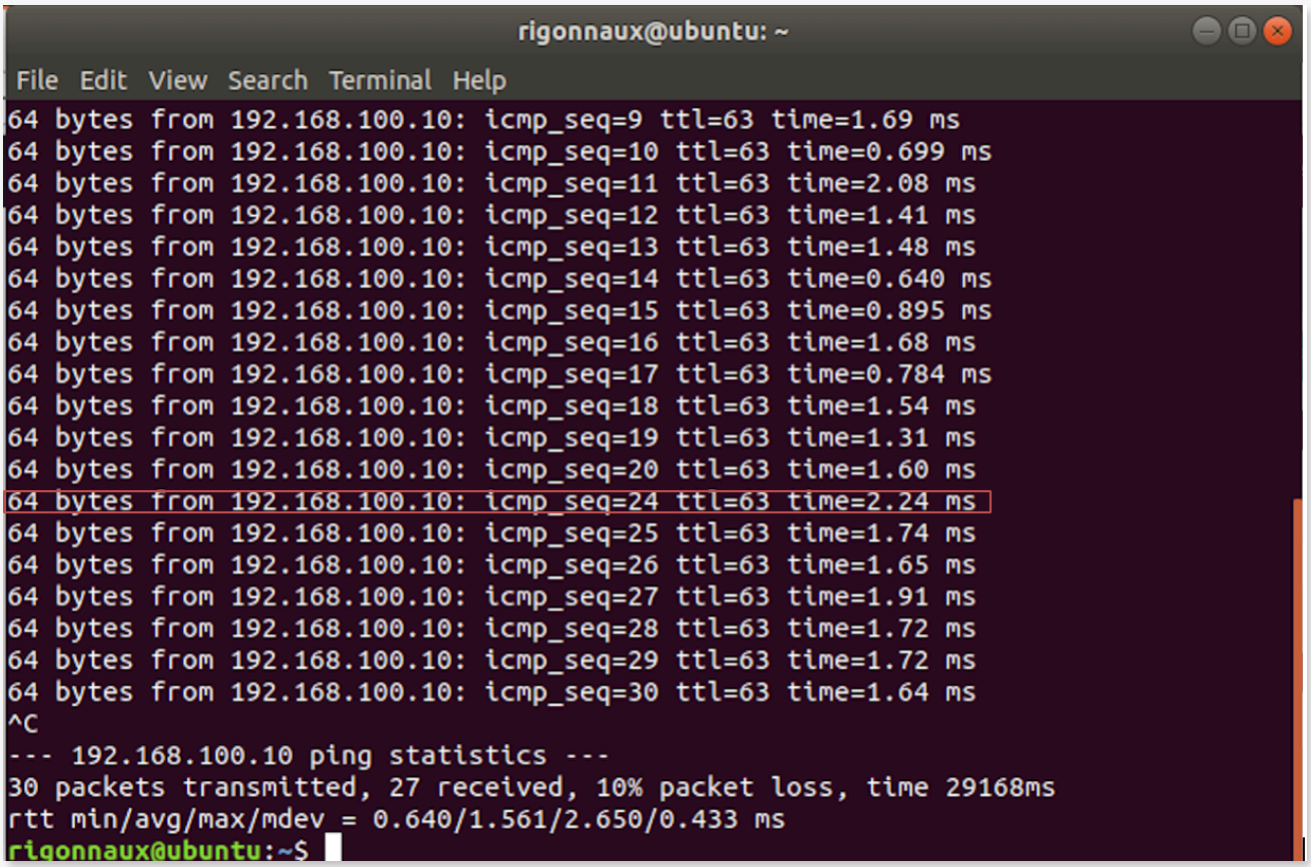


Dans cette partie il sera expliqué les différents tests effectués afin de vérifier le bon fonctionnement de la solution. Ces tests auront pour objectif de confirmer le basculement en cas de panne, le rétablissement à l'ordre prioritaire lors de la correction de la panne, de vérifier la synchronisation des règles, confirmer l'utilité de pfSync, constater le niveau de sécurité des communications.

Test de basculement

Le premier test de cette partie est élémentaire, il consiste à réaliser une simulation de panne permettant de vérifier le bon fonctionnement du procédé de haute-disponibilité et ainsi garantir la continuité de service. Pour se faire il suffit simplement de désactiver le master et de rendre compte du basculement.

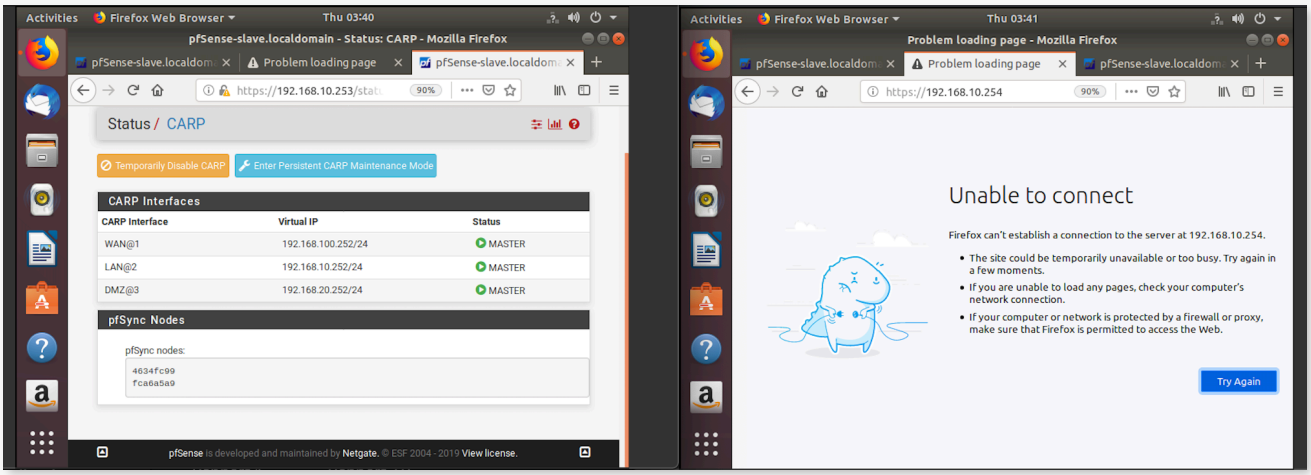
Panne du Firewall PFSense 01 :



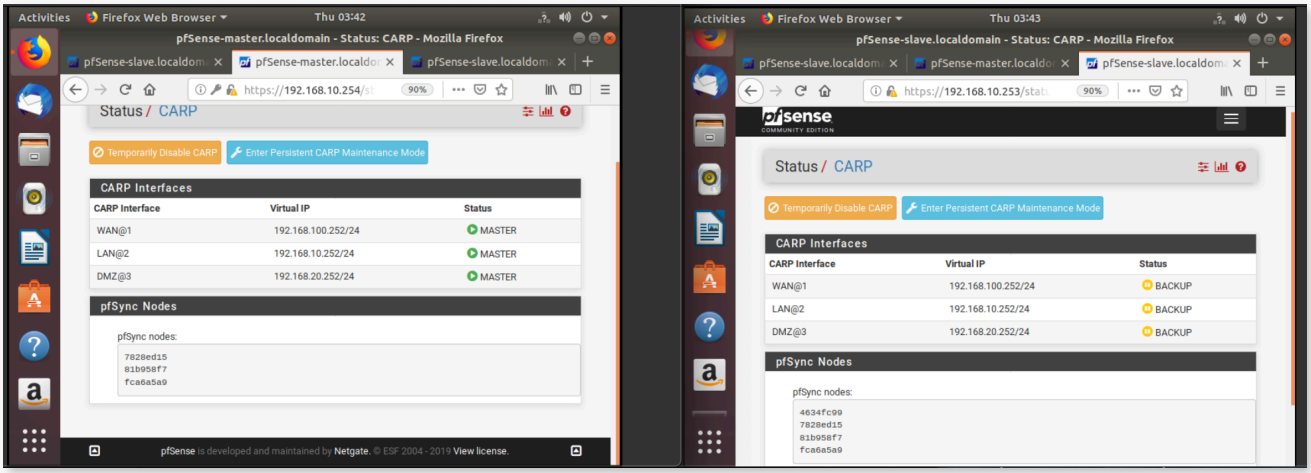
La capture d'écran ci-dessus représente un ping en continu réalisé depuis la machine d'administration présente sur le réseau « LAN » vers le serveur de ressources disponible sur le réseau « WAN ». Le ping est effectué lors de l'arrêt du firewall master, un seul ping obtient un temps de réponse plus important, celui-ci intervient lors du basculement Master/Slave. La continuité de service est donc assurée.

Test de rétablissement

Le deuxième test consiste en vérifier si le rétablissement de l'ordre prioritaire s'effectue correctement. Pour se faire il suffit simplement de redémarrer la machine master originel et d'observer le résultat.



On constate ici que le firewall Master originel est down et que le service est effectif sur le firewall Slave



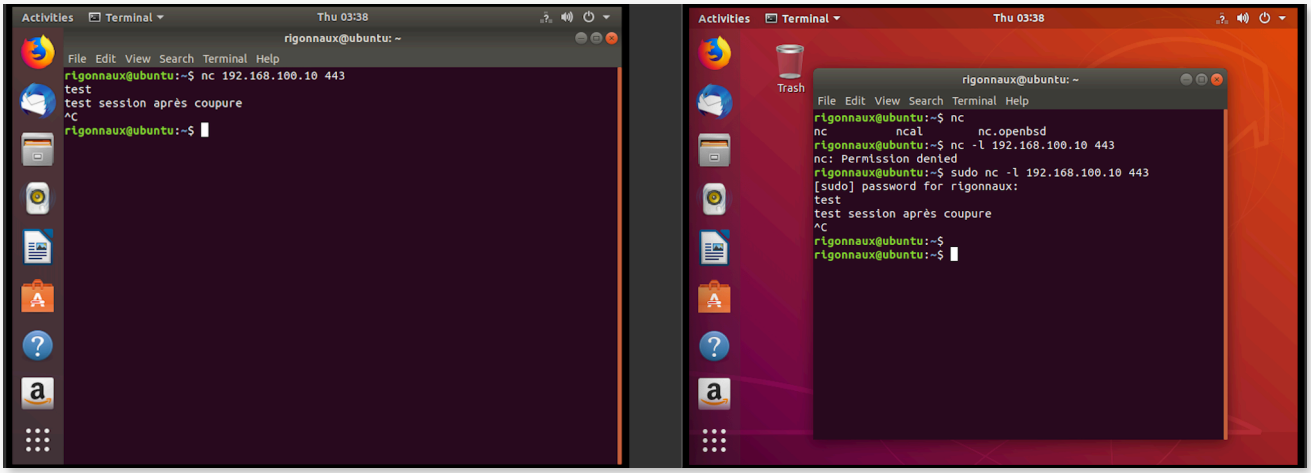
Cette seconde capture prouve que le firewall 01 à repris son rôle de master et le firewall 02 son rôle de backup.

Synchronisation des règles

Un troisième test a été réalisé afin de prouver la prise en compte des nouvelles règles créées lors d'une panne ou d'une maintenance. Dans cette optique le firewall master est donc désactivé, une nouvelle règle est écrite durant cette désactivation, le firewall master est rétablit, si le test est concluant alors la nouvelle est prise en compte.
Aussi lors de la création d'une règle sur le firewall Master cette même règle est automatiquement copié sur le firewall Slave.

Vérification du maintien de session (pfSync)

Afin de certifier une continuité d'activité réellement opérationnelle, un quatrième test est donc réalisé. Celui-ci à pour but de vérifier le maintien d'une session client lors d'un basculement et ainsi prouver la transparence pour l'utilisateur. Il faut dans un premier temps établir un échange, dans notre cas nous avons utilisé le service « netcat » entre le serveur de ressources et la machine d'administration afin de simuler un échange. Ensuite il faudra désactiver le firewall master pour enfin s'assurer que la session est toujours effective. En désactivant pfSync une interruption intervient lors des échanges.



Sécurité des communications

Pour finir afin de s'assurer que les communications entre le maitre et l'esclave sont bien sécurisées nous avons réalisé une capture Wireshark nous permettant d'identifier l'ensemble des types de communications et d'en vérifier leur niveau de sécurité.
On peut donc constater que le protocole XMLRPC est bien chiffré en https, aussi on peut remarquer lors de ces analyses que le protocole CARP est toujours désigné comme étant le protocole VRRP car très proche de celui-ci.

L'ensemble de ces tests nous permettent donc de valider l'ensemble des demandes faites pas le Campus Ynov d'Aix-en-Provence.

YNOV CAMPUS