CPAM Ardèche / Greta Ardèche-Drôme

Pfsense et HighAvailability

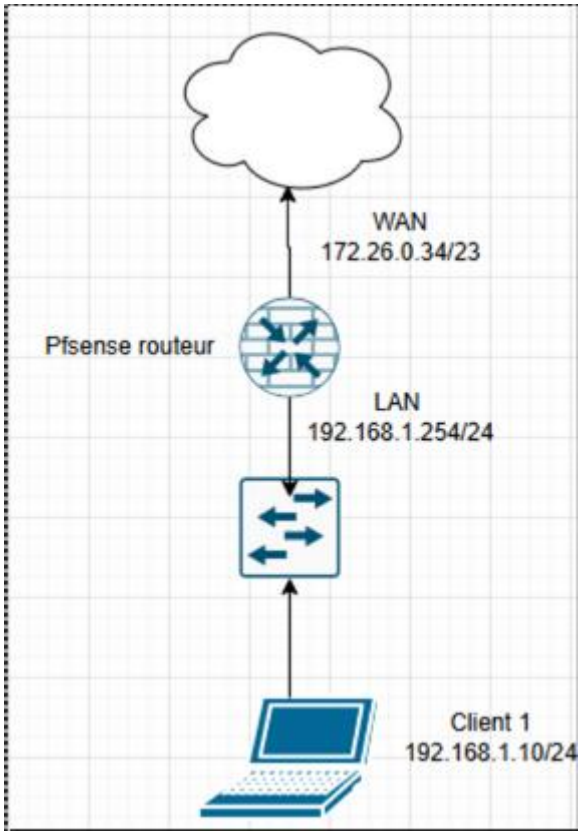
TP

Collet Valentin
BTS SIO-SISR / Session 2026

SOMMAIRE

Cahier des charges

Descriptifs de l'existant



L'infrastructure actuelle comporte seulement un PfSense qui sert de routeur, relié à un switch avec un sous-réseau pour les postes clients.

Sinon, j'ai à disposition dans le cadre de ce TP d'un accès aux machines du GRETA avec un hyperviseur type 2 : **VMWARE Workstation**. Pour les machines, la mienne est équipée de :

- CPU : Intel I7-10700 @ 2.90GHz
- 32 Go RAM DDR4
- 500Go SSD
- 2 cartes réseaux

J'ai déjà l'iso de pfSense à disposition et une VM servant de client.

Besoins

Mettre en place une redondance de Pare-feu pour éviter un single point of Failure (aka SPOF) sur le Firewall.

- Via Connexion direct PFsync entre les deux Pare-feu afin que la configuration du pfSense se réplique du master vers le servant.
- Via protocole CARP pour une redondance au niveau LAN (Carp = protocole de redondance).

Pour cela il va falloir mettre en place :

- Deux VM pfSense
- Une connexion directe entre les deux
- Protocole CARP sur LAN1
- Un client W10 pour tester le bon fonctionnement du failover pfSense

Contraintes

A réaliser dans le cadre d'un apprentissage sur un TP de 4h environs. En respectant la doc de pfSense. On parle ici donc principalement de contrainte **temps**.

Ressources

HighAvailability

Stormshield

J'ai eu plusieurs documentations relatives à PfSense que l'intervenant et professeur a mis à notre disposition, de plus j'ai trouvé de la documentation sur Stormshield pour effectuer mes comparaisons de solution.

Enfin je dispose de l'équipement du GRETA ainsi que de leur réseau.

Analyse

Descriptif des solutions

PfSense est une solution open-source de Pare-feu et routeur, issue d'une distribution FreeBSD, qui propose de nombreux services selon le besoin :

- **VPN** (Virtual Private Network) pour permettre des accès à distance entre des périphériques qui ne sont pas sur le même réseau local.
- **NAT** (Network Address Translation) : qui permet à plusieurs appareils de partager une adresse IP en contrepartie du manque croissant d'adresse ipv4, le routeur (ici

PfSense) va remplacer l'adresse IP source par sa propre IP et inversement en cas de réception.

- **Routage** ce pare-feu peut aussi servir de routeur, il propose des solutions de redondance avec une possibilité de multiplier les liens WAN, et ainsi aussi faire de l'équilibre de charge.
- **Pare-feu** : règles de pare-feu comme le filtrage IP, l'administration des ports, protocoles, etc...
- **Multiples services :** DHCP, Snort, proxy, et autres...

Cette solution est donc basée sur FreeBSD est nécessite donc une VM dédiée à configurer côté serveur, enfin il propose une interface WEB pour l'administration. Il dispose aussi d'une option **d'High Avalaibility** (HA)qui permet d'éviter un SPOF en cas de panne sur un des pare-feu, cette solution d'HA se base sur deux protocoles : **CARP** (qui permet la mise en place d'un lien entre deux pfSense, un côté master et un côté backup, pour que le backup reprenne le relais en cas de panne sur le master) et **Pfsync** (gère la réplication de la configuration du pfSense master vers le pfSense standby).

Stormshield Network Security est lui aussi un pare-feu cette fois sous licence et avec pare-feu matériel. Elle dispose d'un Firewall avec des possibilités exhaustives (IPS, antivirus, filtrage URL, contrôle des applicatifs, segmentation du réseau etc...), de plus son grand avantage est que cette solution a plusieurs **certification**s qui renforcent sa crédibilité dans le domaine de la sécurité. Cette solution est dite « clé en main », le déploiement est donc simplifié et ne nécessite pas de compétence côté serveur linux.

Comparaison des solutions :

	PfSense	Stormshield	Analyse
Coût	Open-source (gratuit)	License et matériel	Ici la solution la plus économique est donc PfSense
High-availability	CARP et Load balancing possible des liens WAN	Deux méthode d'HA : actif/passif (supervision du pare-feu maître par le pare-feu passif qui prend le relais) et actif/actif (partage de charge). Possibilité de multiple lien WAN aussi.	RAS
Modularité	PfSense est très flexible grâce à la possibilité d'ajout de plugins	Non, mais est livré avec beaucoup de service de base	Ici PfSense est plus facilement personnalisable selon les besoins.
Ergonomie	Nécessite des compétences en réseau pour la mise en place et l'entretien	Solution accessible	D'un point de vue accessibilité Stormshield est la solution la plus intéressante
Certification	Aucune	ANSSI / EAL4+ / OTAN	Stormshield est ici une garantie au niveau sécurité de par ses certifications.

Choix d'une solution

Des études précédentes on remarque que PfSense :

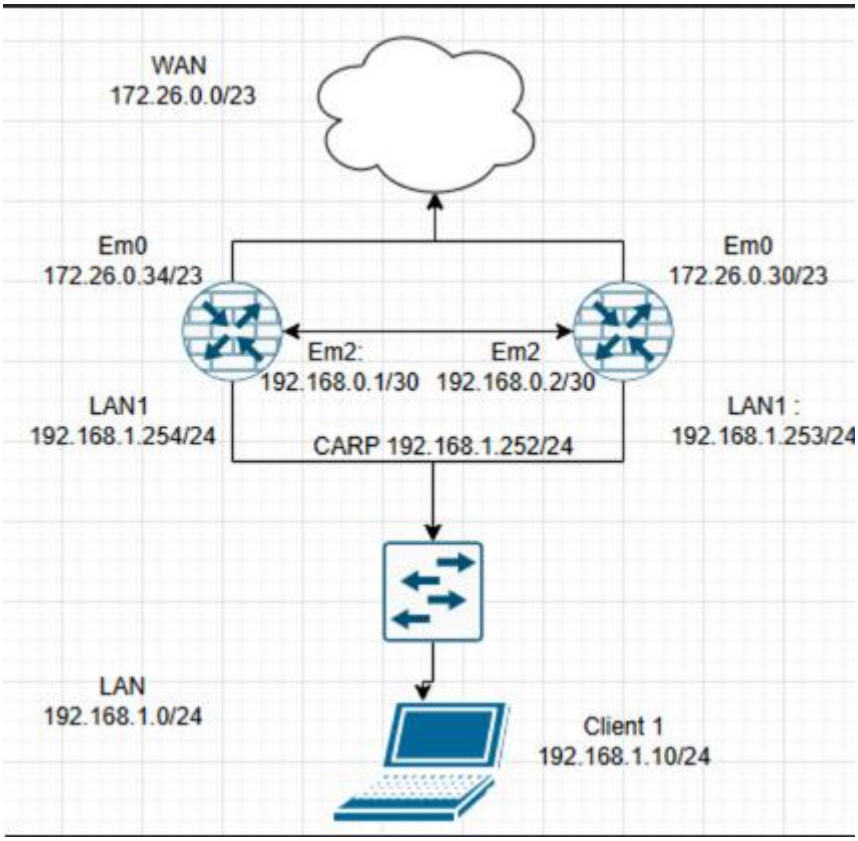
- Est plus adapté à des petits ou moyen réseau
- Est plus flexible
- Est aussi plus adapté à un environnement avec des exigences de sécurité moindre.
- S'adresse à des personnes compétentes en administration réseau, avec des connaissances en Linux et FreeBSD.

Tandis que Stormshield lui :

- S'adresse plus facilement à un grand réseau d'entreprise, qui nécessite des garanties de sécurité importantes.
- Il est plus facilement mis en place et administrable.

Dans ce contexte (en plus de celui du TP), je vais me diriger vers pfSense qui répond donc à nos besoins actuels.

Plan d'adressage et schéma



Etude de l'impact sur le SI existant

Au niveau **Technique** : la redondance du pare-feu va éviter ainsi un SPOF sur le pare-feu avec un deuxième pfSense qui prend le relais, pour cela la config du pfSense est répliqué via pfsync et le Protocol CARP permet une redondance au niveau du Lan.

Au niveau **Humain**: il est nécessaire de former les équipes à l'utilisation du pare-feu, assez complexe par sa grande modularité.

Au niveau **coût** cette solution est open source et représente donc une économie.

Phasage de l'intervention et prévision des tests :

- Configuration pfSense 1 et 2
  - Interface Wan + Lan + opt1
- Configuration pfsync + XMLRPC (XMLRPC seulement sur pfSense 1)
- Configuration des règles de pare-feu sur pfSense 1 & 2
  - ☐ Protocole TCP port 443 (HTTPS)
    - **Test** : recherche web sur un site HTTPS
  - ☐ Protocole Pfsync
- **Test** de bon fonctionnement du pfsync (ajouter une règle pare-feu et vérifié sa réplication sur le pfSense II)
- Configuration CARP sur pfSense 1 & 2
- Configuration client Windows 10 sur passerelle CARP
- **Test** du protocole CARP
  - ☐ Pause du pfSense master
  - ☐ Ping 8.8.8.8 avec client

Déploiement

Déploiement le 13.02.25, de 8h -12h et 13h30 – 17h30

Mise en place

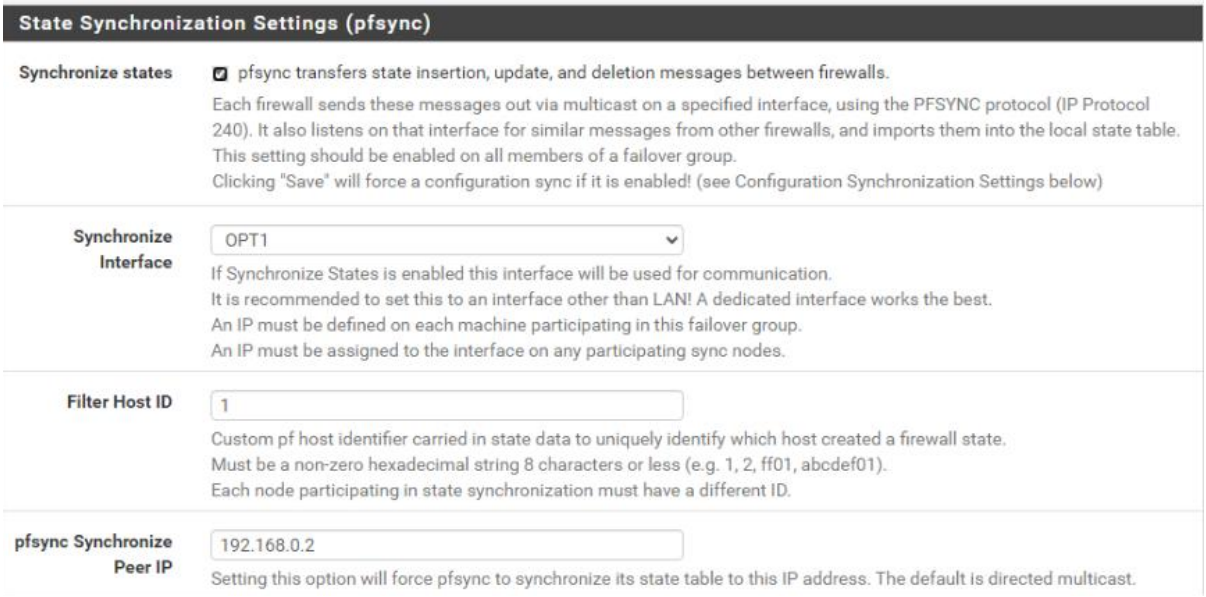
1. Réglage configuration réseau pfSense 1 et 2 :

a.
```
WAN (wan)       -> em0       -> v4/DHCP4: 172.26.0.34/23
LAN (lan)       -> em1       -> v4: 192.168.1.254/24
OPT1 (opt1)     -> em2       -> v4: 192.168.0.1/30
```

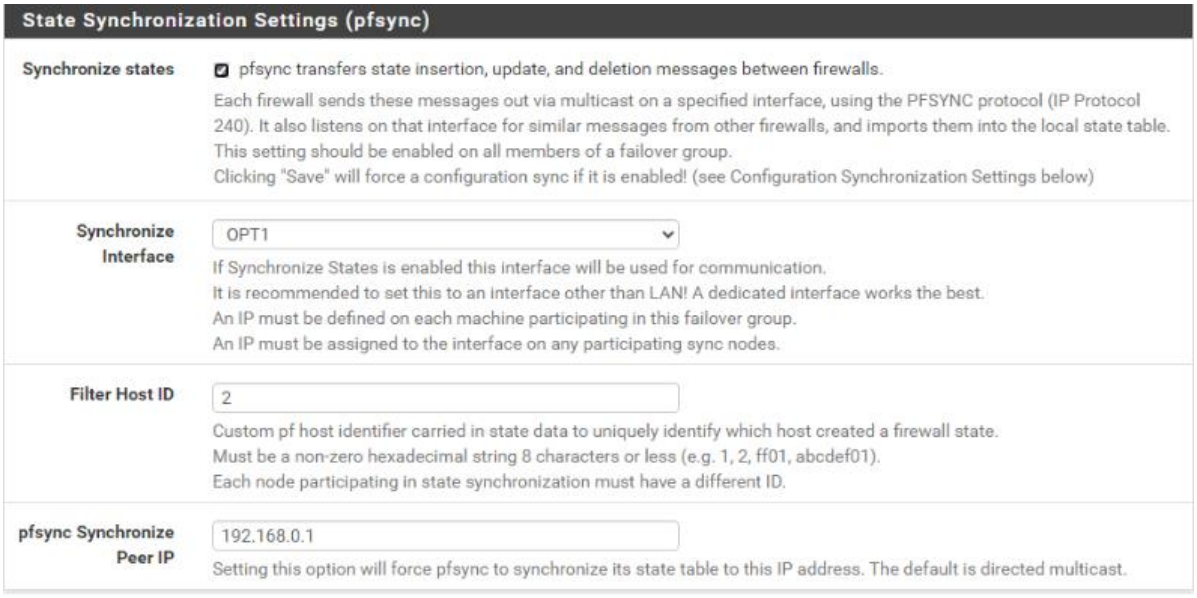
b.
```
WAN (wan)       -> em0       -> v4/DHCP4: 172.26.0.30/23
LAN (lan)       -> em1       -> v4: 192.168.1.253/24
OPT1 (opt1)     -> em2       -> v4: 192.168.0.2/30
```

2. Réglage du Pfsync 1 & 2

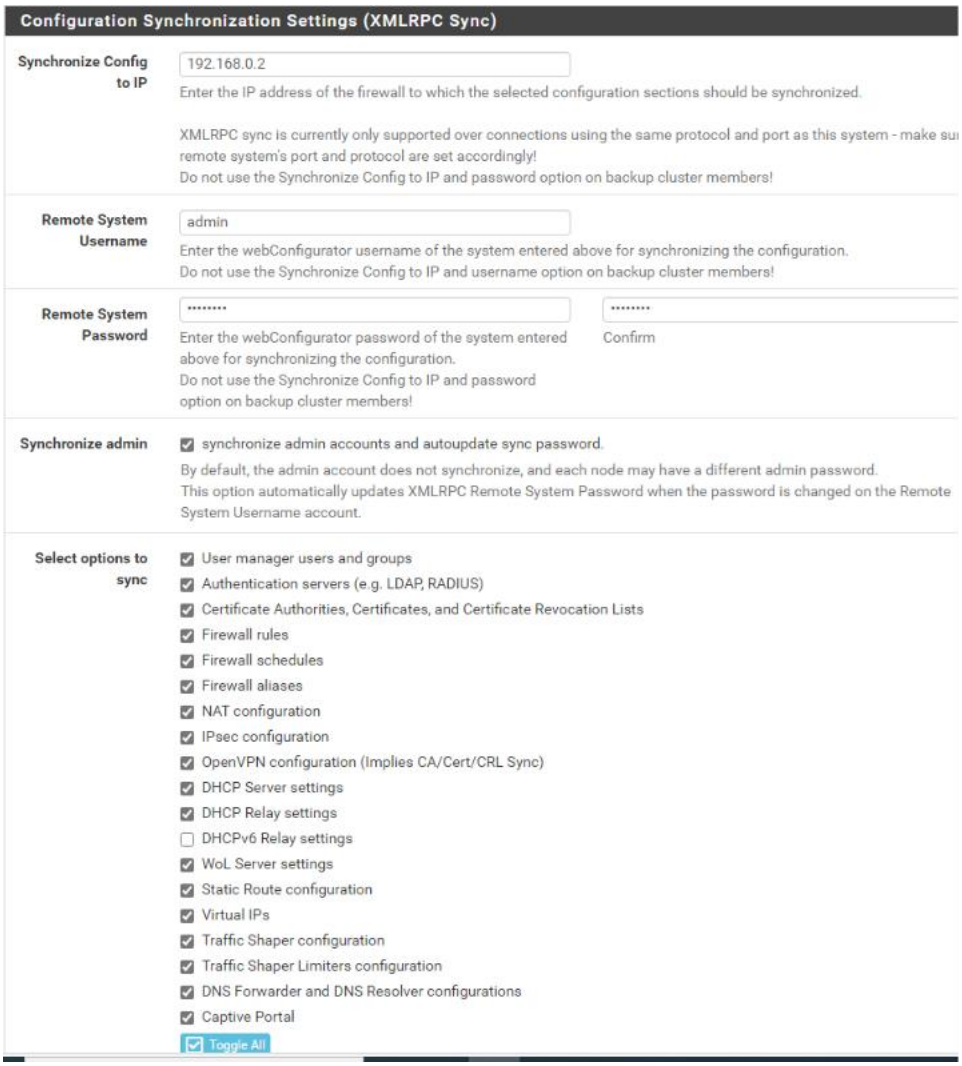
a.


State Synchronization Settings (pfsync)
Synchronize states
pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface
OPT1
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.
Filter Host ID
1
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
Each node participating in state synchronization must have a different ID.
pfsync Synchronize Peer IP
192.168.0.2
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

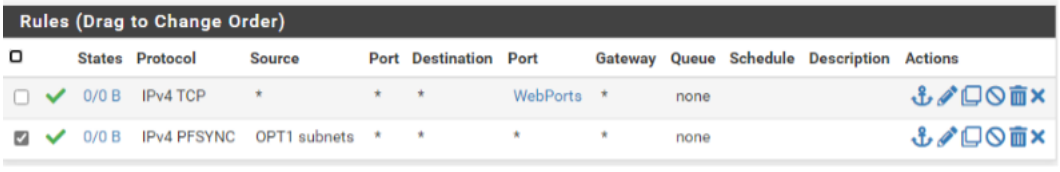
b.


State Synchronization Settings (pfsync)
Synchronize states
pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface
OPT1
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.
Filter Host ID
2
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
Each node participating in state synchronization must have a different ID.
pfsync Synchronize Peer IP
192.168.0.1
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

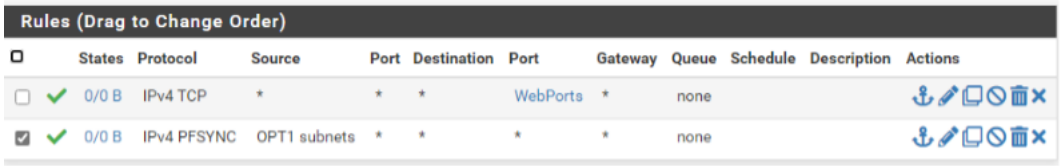
3. Configuration XMLRPC sync sur pfsense 1 :

a. 

4. Configuration règles pare-feu

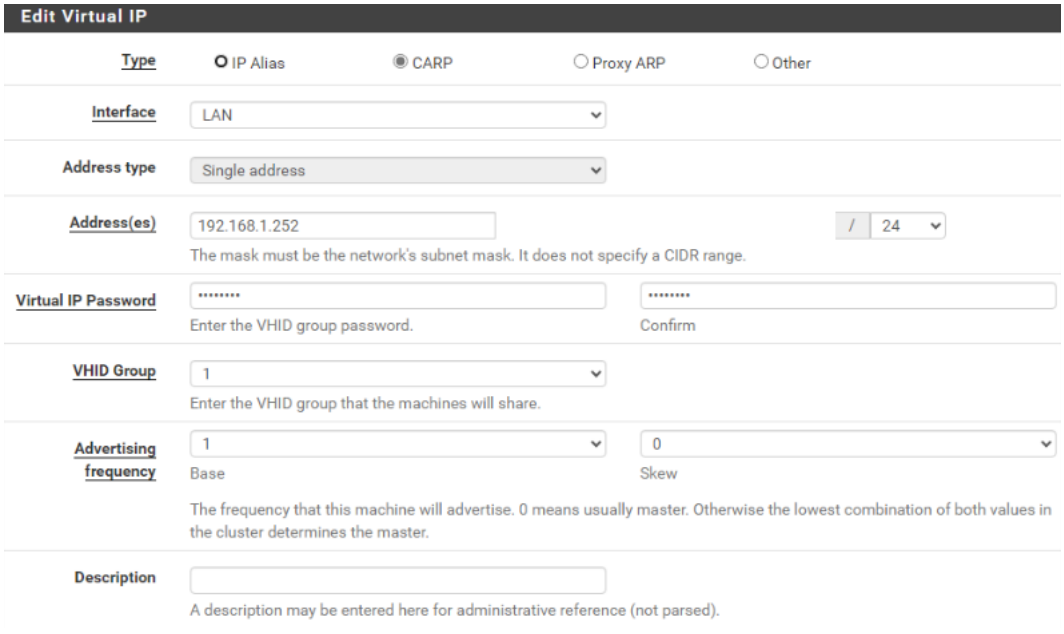
a. 

b. Test réplication d'une règle pare-feu sur pfsense 1 (type ICMP4) : la règle se réplique correctement sur le pfsense 2

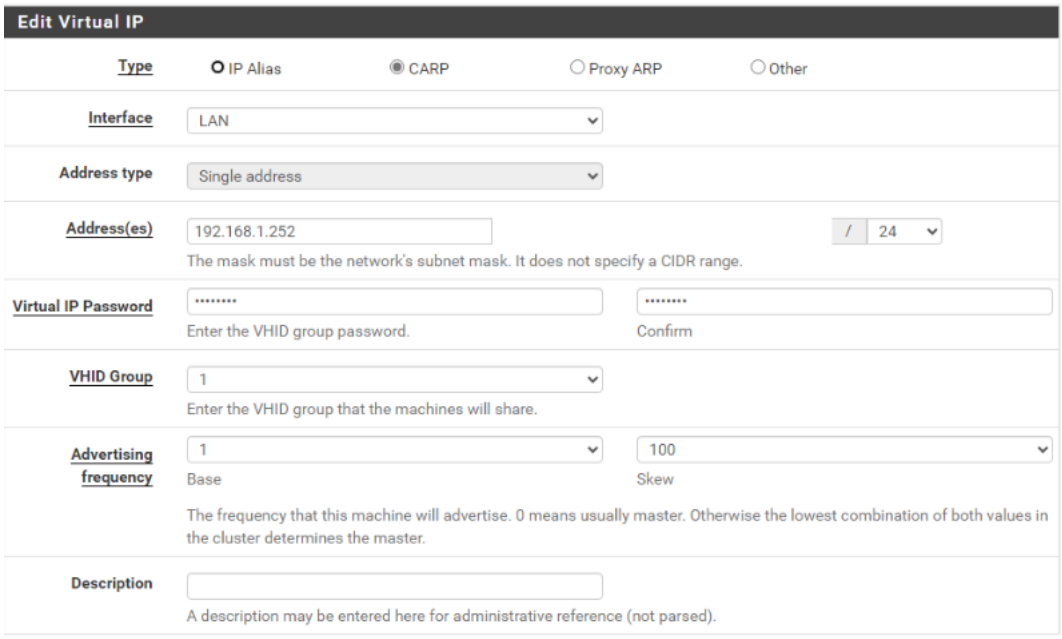


5. Configuration CARP

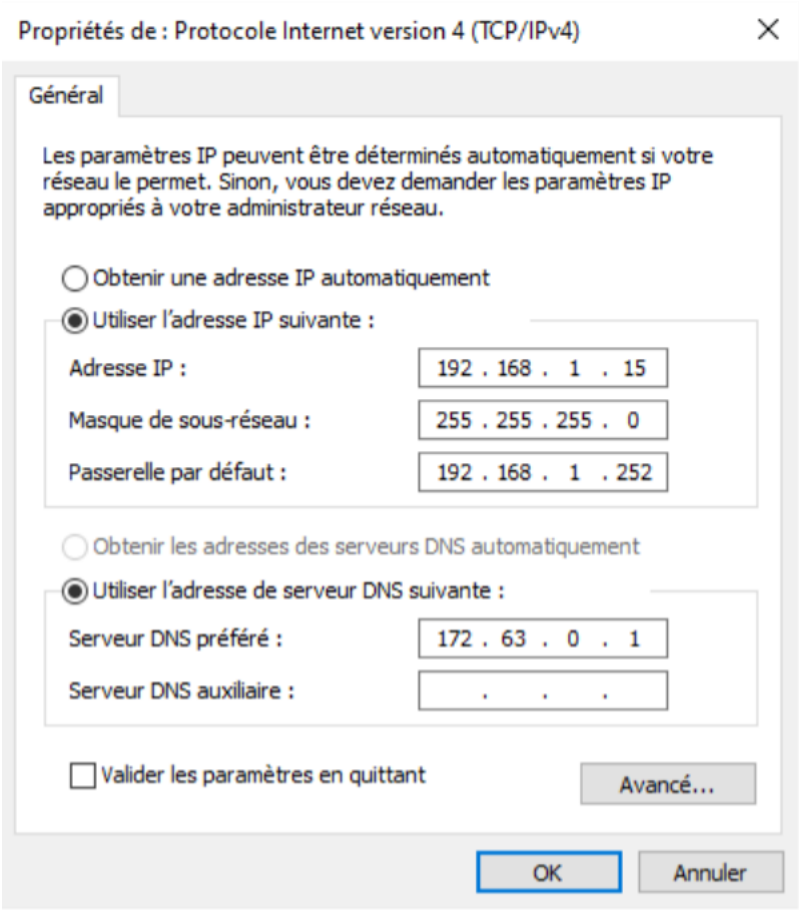
a.



b.



c. Configuration Gateway CARP sur client



d. Déconnexion du pfSense master

e. Le pfSense 2 prend le relais du pfSense master, le client PC arrive toujours à joindre le WAN.

```
C:\Users\Telloc>ping 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=111

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 10ms, Moyenne = 9ms
```

Rapport de tests

Les tests sont inclus dans le déploiement, ils vont principalement consistés à vérifier que le pfSense en standby réplique bien la configuration du master, par la suite qu'il prenne le relais en cas où le pfSense master est down.

Rapport de déploiement

Le déploiement s'est correctement fait, le pfsync est fonctionnel, et en cas de chute du pfSense master le pfSense standby prend le relais.

Bilan

Conclusion :

La mise en place du pare-feu en redondance est effectuée et fonctionnelle, le réseau sera donc toujours protégé même si le premier boîtier pfSense dysfonctionne en évitant ainsi un SPOF. De plus, ce deuxième pare-feu en redondance réplique les mêmes règles de pare-feu et configuration que le pfSense 1.

Auto-évaluation :

Je peux progresser sur la lecture de la documentation officielle (typiquement en lisant les rubriques qui concernent ma problématique avant de me lancer dans la configuration et d'adapter celle-ci au fur et à mesure de la documentation, afin d'avoir une meilleure vue d'ensemble directement sur le projet). Ainsi la configuration du pfsync aurait été facilitée.