BTS Services informatiques aux organisations- SISR

Session 2025

E5 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- **Layer Bureautique et Informatique** est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.
- La problématique principale réside dans le besoin garantir une **haute disponibilité** de ses services informatiques pour l'ensemble de ses utilisateurs. Afin d'assurer la continuité d'activité, tous les services doivent rester accessibles à tout moment, sans interruption, même en cas de défaillance d'un composant réseau clé, tel qu'un pare-feu.
- La solution choisie consiste à déployer un second pare-feu pfSense pour assurer la haute disponibilité (HA) du réseau. Grâce à l'utilisation d'adresses IP virtuelles (VIP), de la synchronisation pfsync et du service CARP, la continuité d'accès aux services est garantie en cas de défaillance d'un équipement.

Intitulé de la réalisation professionnelle

Haute disponibilité réseau : installation d'un cluster pfSense

Période de réalisation : 20/08/24- 21/08/24 **Lieu :** AUXERRE

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

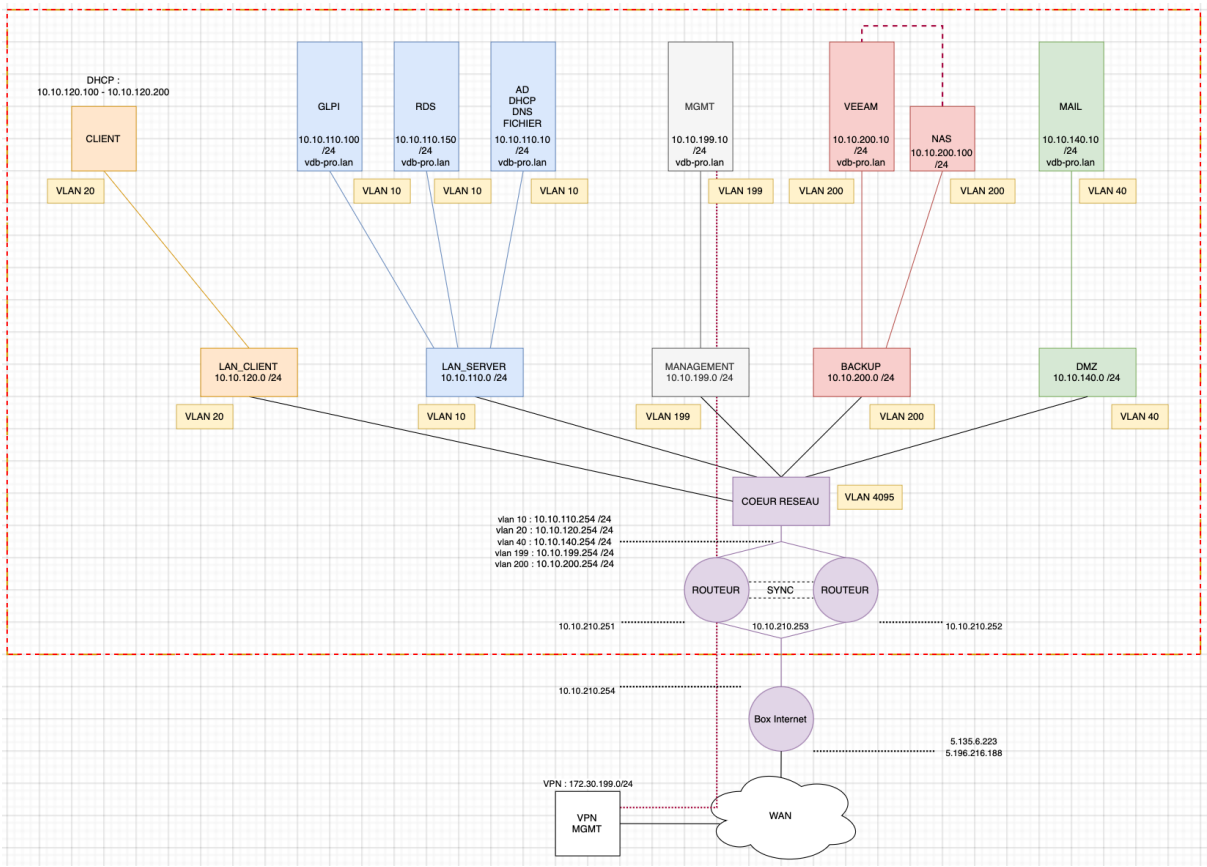
- **Ressources disponibles (Situation avant RP)**
  L'infrastructure disposait d'un serveur ESXi opérationnel pour l'hébergement des différents services de l'entreprise. Un seul pare-feu pfSense était en place pour gérer l'ensemble des flux réseau, assurer la sécurité et garantir la disponibilité des services.
- **Résultats attendus (Situation après RP)**
  Après la mise en place de la haute disponibilité avec pfSense, le réseau de l'entreprise reste opérationnel même en cas de panne d'un pare-feu, grâce à une bascule automatique et transparente, garantissant ainsi une continuité d'accès aux services.
- **Durée de réalisation**
  L'intervention a duré 2 jours, comprenant l'installation, la configuration, la sécurisation ainsi que la phase de tests de la solution. La partie la plus longue a été la gestion des différents réseaux un par un afin d'éviter toute coupure générale des services et ainsi prévenir un arrêt de la production.

Modalités d'accès à cette réalisation professionnelle.

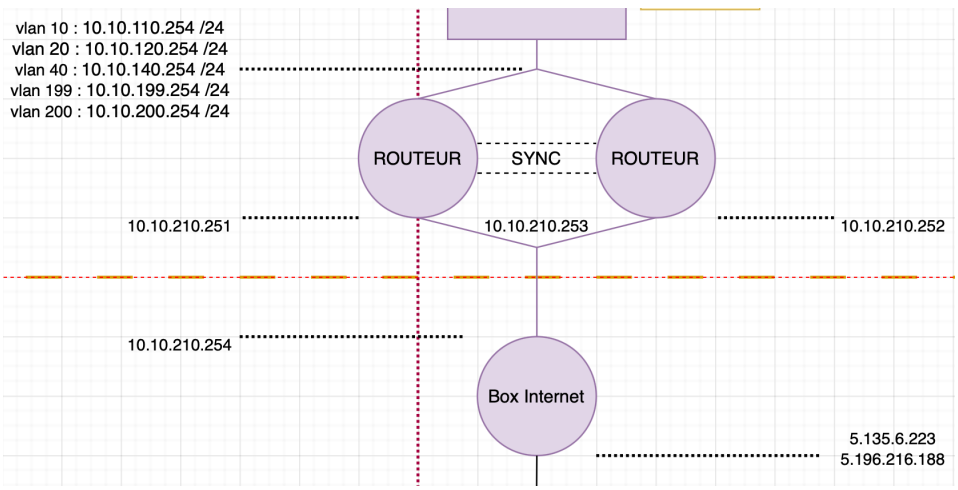
https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission, j'ai réalisé un projet professionnel visant à assurer la haute disponibilité du réseau de l'entreprise. Pour cela, j'ai déployé une solution basée sur pfSense en mode CARP, permettant la mise en place d'un cluster de pare-feux pour garantir la redondance et la continuité des services. Ce projet m'a permis de développer des compétences en gestion de réseau, administration de pare-feu, sécurité des infrastructures et haute disponibilité.



L'élément le plus important dans ce schéma est la partie réseau, en particulier l'intégration des pare-feux pfSense.



Configuration du premier PfSense

Je commence par me connecter au premier pfSense déjà en place. Je configure les adresses IP de toutes les interfaces en terminant par .251, ce qui permet de mémoriser facilement qu'il s'agit du pfSense principal (pfSense 1 = .251). J'ajoute ensuite une nouvelle interface nommée **SYNC**, dédiée à la synchronisation entre les deux pfSense. Cette interface permet de répliquer automatiquement la configuration via le service **pfsync**.

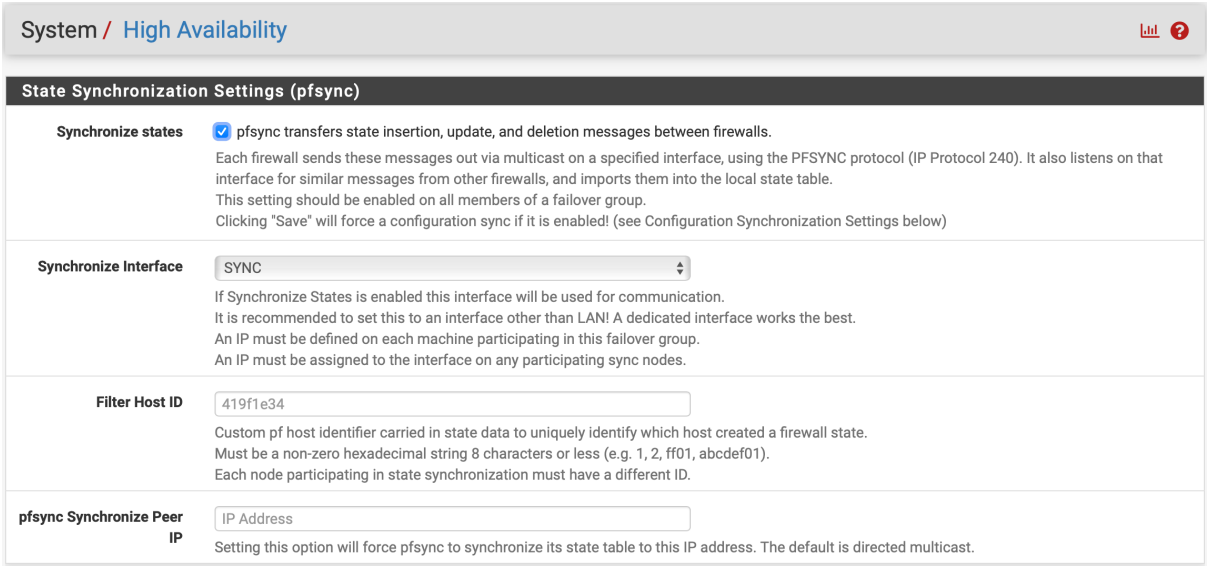
Interfaces			
WAN	↑	autoselect	10.10.210.251
LAN	↑	autoselect	n/a
VLANSERVER	↑	autoselect	10.10.110.251
VLANCLIENT	↑	autoselect	10.10.120.251
VLANDMZ	↑	autoselect	10.10.140.251
VLANMGMT	↑	autoselect	10.10.199.251
VLANBACKUP	↑	autoselect	10.10.200.251
SYNC	↑	autoselect	172.29.100.251

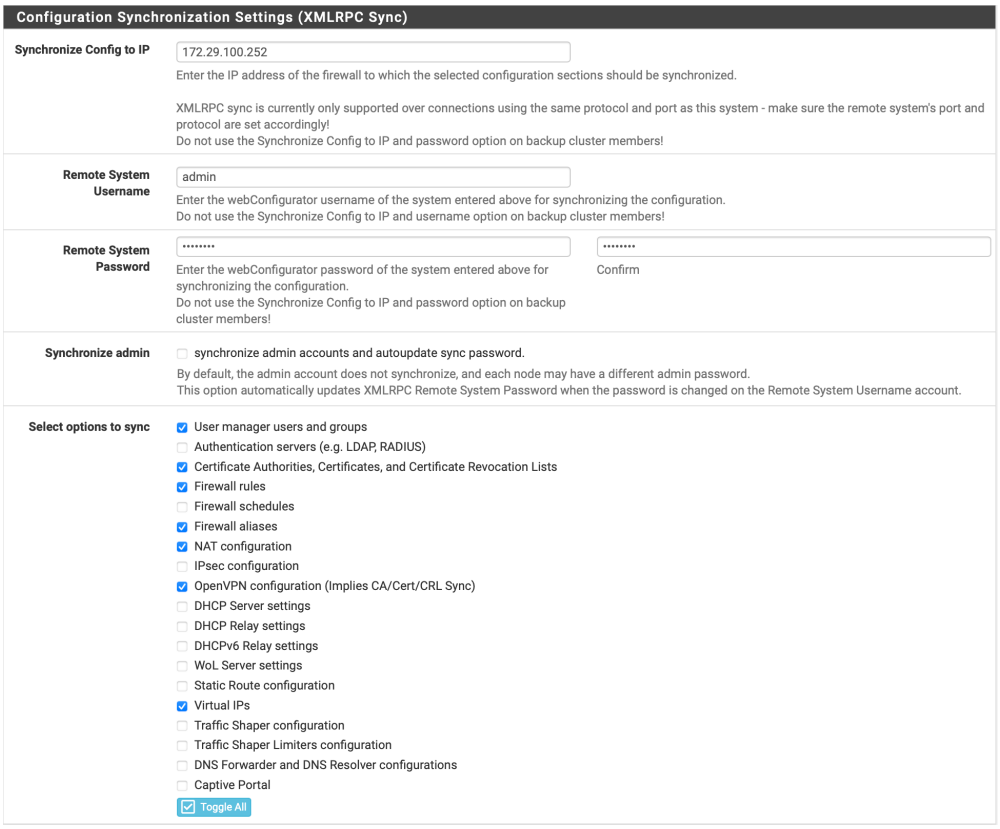
Une fois les interfaces créées sur le premier pfSense, j'ajoute les mêmes interfaces, nommées à l'identique, sur le second pfSense, en particulier l'interface **SYNC**. Celle-ci est essentielle pour mettre en place la synchronisation en temps réel entre les deux pare-feux. Grâce à cette configuration, toute modification effectuée sur le pfSense principal est automatiquement répliquée sur le second, ce qui permet d'éviter une double saisie et assure une cohérence parfaite entre les deux systèmes.

Interfaces			
WAN	↑	autoselect	10.10.210.252
LAN	↑	autoselect	n/a
VLANSERVER	↑	autoselect	10.10.110.252
VLANCLIENT	↑	autoselect	10.10.120.252
VLANDMZ	↑	autoselect	10.10.140.252
VLANMGMT	↑	autoselect	10.10.199.252
VLANBACKUP	↑	autoselect	10.10.200.252
SYNC	↑	autoselect	172.29.100.252

Mise en place du Pfsync

Je configure la synchronisation entre les deux pfSense à l'aide de **pfsync**. Comme mentionné précédemment, il est essentiel que les interfaces soient identiques et nommées de la même manière sur les deux pare-feux, sans quoi la synchronisation ne fonctionnera pas correctement. La configuration s'effectue depuis l'onglet **High Availability Sync** sur le pfSense principal (ici, le pfSense 1). On y sélectionne l'interface dédiée à la synchronisation (dans notre cas, **SYNC**), puis on renseigne l'adresse IP du pfSense secondaire, ainsi que les identifiants (login/mot de passe) permettant la connexion. Enfin, il est recommandé de sélectionner uniquement les éléments réellement utilisés pour éviter des erreurs ou conflits lors de la synchronisation.





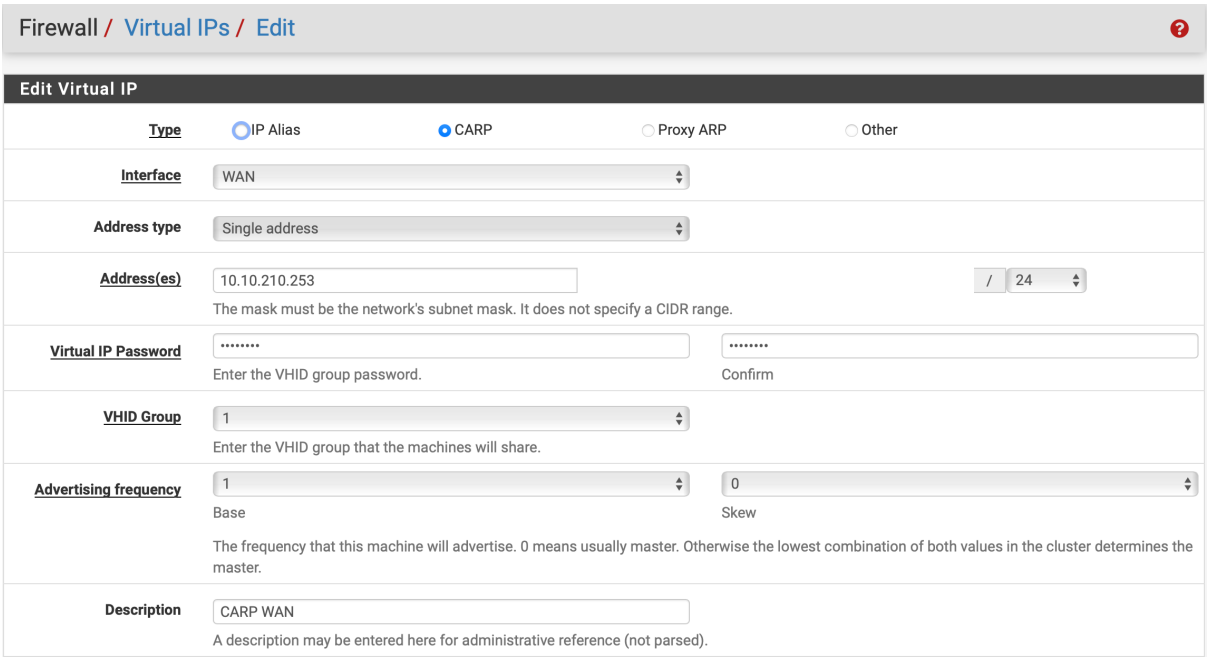
Mise en place des IP virtuelles (VIP) et du service CARP

Maintenant que la synchronisation entre les deux pfSense est opérationnelle, il est possible de tout configurer directement depuis le pfSense principal, les changements étant automatiquement répliqués sur le second.

L'étape suivante consiste à créer des **adresses IP virtuelles (VIP)**, nécessaires pour activer le service **CARP**. Ce service permet la mise en place d'un système de **failover** : en cas de panne du pfSense principal, le second prend immédiatement le relais, assurant ainsi une redondance automatique. On parle alors de bascule : le pfSense secondaire devient maître (Master), tandis que l'autre passe en mode secours (Backup). Une fois le pfSense principal à nouveau fonctionnel, il reprend automatiquement son rôle de maître.

Pour que ce mécanisme fonctionne correctement, un système de **priorités** est défini, permettant à chaque pare-feu de savoir s'il doit être maître ou backup selon la situation.

Il est important de noter que lorsque l'option **pfsync** est activée, le pfSense maître se voit automatiquement attribuer une priorité plus élevée que le pfSense en mode backup, ce qui garantit un comportement logique lors des bascules.



Une fois toutes les **adresses IP virtuelles (VIP)** correctement configurées, il est possible de vérifier l'état du service **CARP** via l'interface d'administration afin de s'assurer que la redondance est bien active et fonctionnelle.

Firewall / Virtual IPs

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
10.10.210.253/24 (vhid: 1)	WAN	CARP	CARP WAN	
10.10.110.254/24 (vhid: 2)	VLANSERVER	CARP	CARP SERVER	
10.10.120.254/24 (vhid: 3)	VLANCLIENT	CARP	CARP CLIENT	
10.10.140.254/32 (vhid: 4)	VLANDMZ	CARP	CARP DMZ	
10.10.199.254/24 (vhid: 5)	VLANMGMT	CARP	CARP MGMT	
10.10.200.254/24 (vhid: 6)	VLANBACKUP	CARP	CARP BACKUP	

pfSense 1 (Maitre) :

Status / CARP

CARP Maintenance

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	10.10.210.253/24	CARP WAN	MASTER
VLANSERVER@2	10.10.110.254/24	CARP SERVER	MASTER
VLANCLIENT@3	10.10.120.254/24	CARP CLIENT	MASTER
VLANDMZ@4	10.10.140.254/32	CARP DMZ	MASTER
VLANMGMT@5	10.10.199.254/24	CARP MGMT	MASTER
VLANBACKUP@6	10.10.200.254/24	CARP BACKUP	MASTER

pfSense 2 (Backup) :

Status / CARP

CARP Maintenance

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

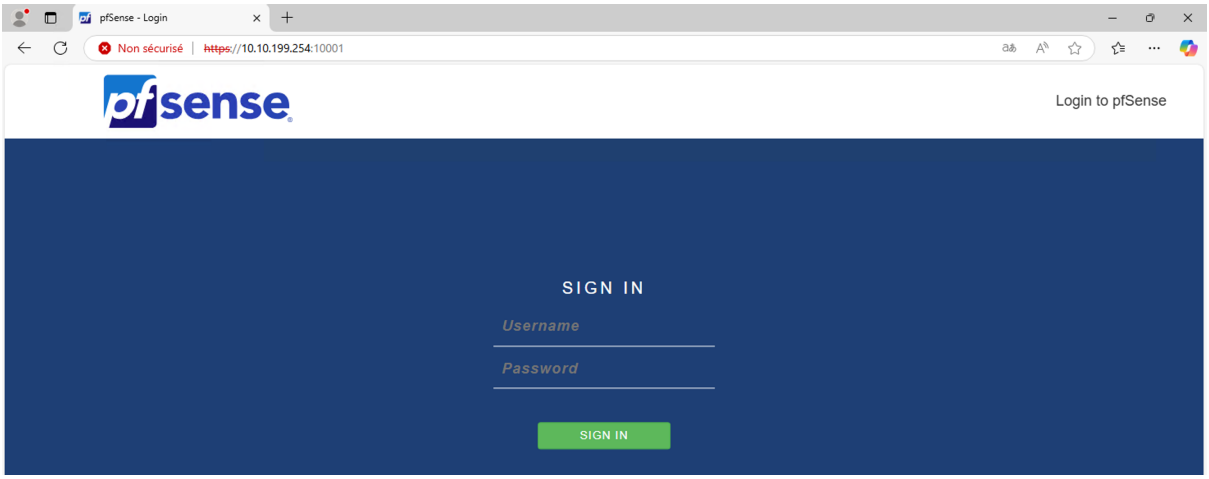
CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	10.10.210.253/24	CARP WAN	BACKUP
VLANSERVER@2	10.10.110.254/24	CARP SERVER	BACKUP
VLANCLIENT@3	10.10.120.254/24	CARP CLIENT	BACKUP
VLANDMZ@4	10.10.140.254/32	CARP DMZ	BACKUP
VLANMGMT@5	10.10.199.254/24	CARP MGMT	BACKUP
VLANBACKUP@6	10.10.200.254/24	CARP BACKUP	BACKUP

Partie 2 – Validation

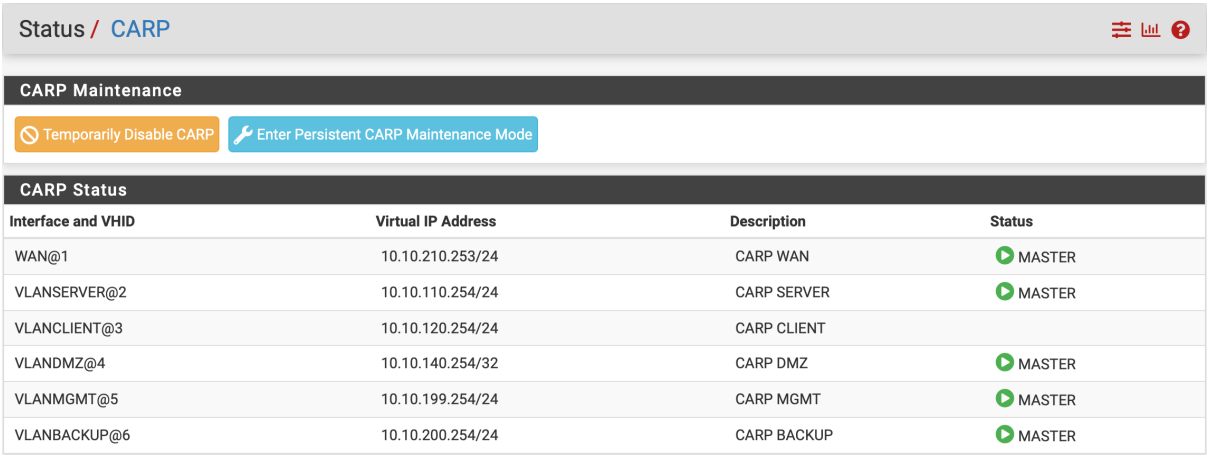
Pour valider le bon fonctionnement de la synchronisation **pfsync**, il suffit de créer une règle sur le pfSense 1, puis de vérifier que celle-ci est bien répliquée instantanément sur le pfSense 2.

Concernant les **adresses IP virtuelles**, leur fonctionnement peut être testé en se connectant à l'interface d'administration via l'une de ces IP, comme le **VLANMGMT** en **.254**, qui correspond à une IP virtuelle partagée.



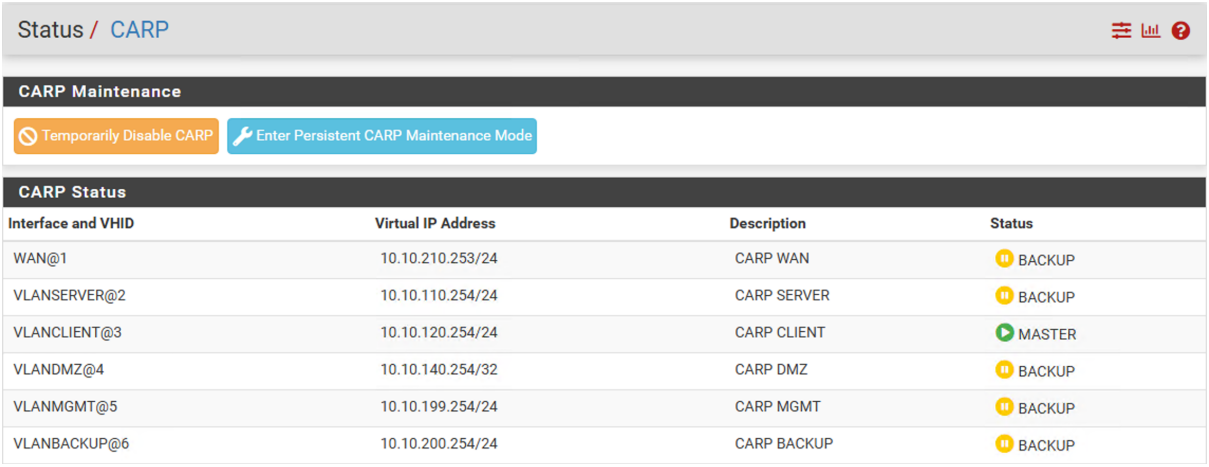
Ensuite, pour tester le service **CARP**, il est possible de désactiver temporairement l'interface **VLANCLIENT** sur le pfSense principal. Cela permet d'observer si le pfSense secondaire prend bien le relais automatiquement sur ce réseau, validant ainsi le mécanisme de bascule.

pfSense 1 : Panne de VLANCLIENT

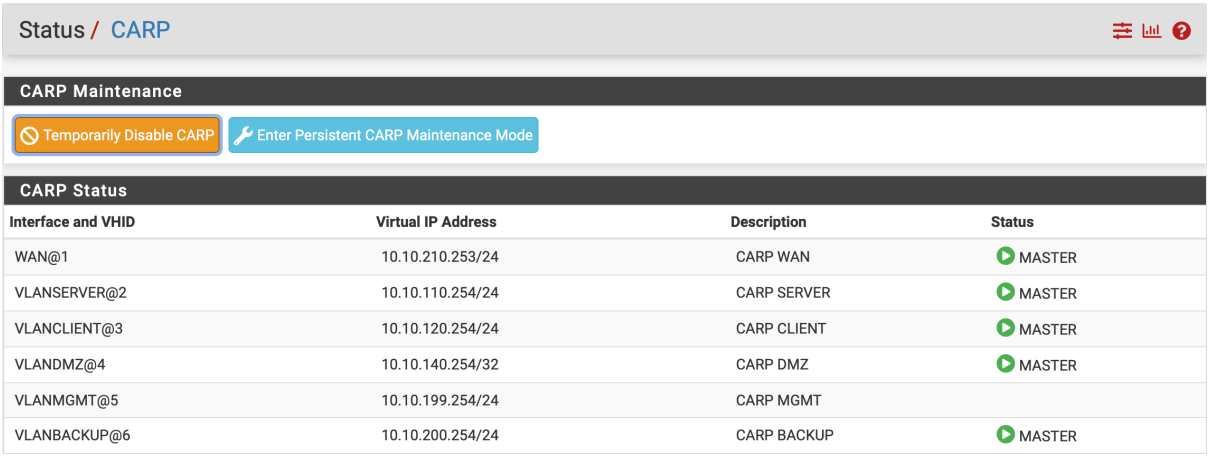


Interface and VHID	Virtual IP Address	Description	Status
WAN@1	10.10.210.253/24	CARP WAN	MASTER
VLANSERVER@2	10.10.110.254/24	CARP SERVER	MASTER
VLANCLIENT@3	10.10.120.254/24	CARP CLIENT	
VLANDMZ@4	10.10.140.254/32	CARP DMZ	MASTER
VLANMGMT@5	10.10.199.254/24	CARP MGMT	MASTER
VLANBACKUP@6	10.10.200.254/24	CARP BACKUP	MASTER

pfSense 2 : Devient « Maitre » de VLANCLIENT



Enfin, pour valider pleinement le fonctionnement du **failover** de pfSense, le test le plus significatif consiste à observer le comportement du trafic en cas de panne du pfSense principal. Pour cela, j'effectue un **ping continu** depuis le poste de management, ce qui permet de mesurer la perte éventuelle de paquets lors de la coupure, ainsi que la reprise du service lorsque le pfSense maître redevient actif.



Après la coupure du pfSense 1, une seule perte de paquet est observée, ce qui reste négligeable et sans impact notable, mis à part une brève déconnexion du VPN, qui se reconnecte automatiquement.

```
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Délai d'attente de la demande dépassé.
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
```

Lorsque le pfSense 1 redevient maître et reprend le contrôle des interfaces, la bascule se fait de manière totalement transparente : aucune perte de paquet n'est constatée, et la reconnexion s'effectue immédiatement, sans que l'utilisateur ne perçoive le moindre changement.

```
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
Réponse de 10.10.110.10 : octets=32 temps<1ms TTL=127
```

Partie 3 – Veille Technologique

Dans le cadre de ce projet, une veille technologique a été réalisée afin d'explorer les différentes solutions existantes en matière de haute disponibilité réseau et de redondance de pare-feux. L'objectif était de comparer pfSense avec d'autres solutions open source ou commerciales telles que OPNsense, FortiGate HA, Sophos ou encore Cisco ASA avec failover.

Cette veille a permis de constater que pfSense, en plus d'être gratuit et open source, offre des fonctionnalités robustes comme CARP, pfsync, et une interface web complète, tout en restant flexible et simple à mettre en œuvre dans un environnement virtualisé. Des recherches ont également été menées sur les bonnes pratiques de configuration, la gestion des priorités CARP, la sécurité des synchronisations inter-pare-feux et la résilience en cas de panne.

La solution pfSense avec CARP présente plusieurs avantages notables : elle est **gratuite**, **open source**, relativement simple à déployer, et permet une **haute disponibilité efficace** grâce à la redondance automatique. L'interface web est intuitive, et les fonctionnalités comme **pfsync** ou les **VIP** facilitent la gestion du cluster. Cependant, cette solution comporte aussi quelques inconvénients, notamment une **configuration sensible** à la cohérence des interfaces, un **manque de support officiel** comparé aux solutions commerciales, et une **documentation parfois dispersée**, ce qui peut rallonger le temps de mise en œuvre en cas de problème.

Lors de ma veille technologique, j'ai également étudié **OPNsense**, une alternative directe à pfSense. Cette solution m'a semblé **très légère, optimisée et stable**, ce qui en fait un excellent choix pour des environnements à faibles ressources. Toutefois, malgré ses atouts techniques, j'ai trouvé son interface **moins intuitive** et **moins conviviale** à mon goût que celle de pfSense, en particulier pour une gestion quotidienne. Ayant été formé sur pfSense depuis longtemps, je suis plus à l'aise avec son environnement, ce qui a naturellement orienté mon choix vers cette solution. Cela dit, je reste **ouvert aux autres technologies** et je teste régulièrement **de nouveaux outils** afin de développer des compétences variées et rester à jour dans le domaine des infrastructures réseau.

Enfin, cette veille a mis en lumière l'importance croissante de la haute disponibilité dans les infrastructures modernes, en particulier avec la montée en charge des services hébergés localement ou en cloud, et les attentes élevées en termes de continuité de service pour les utilisateurs.