REDONDANCE DE PARE-FEU PFSENSE

Cédric BAUDIMENT
AgroMousquetaires – Site d'Antartic 2

BTS SIO SISR
Greta Drôme / Ardèche
2024 / 2026

I/ Cahier des charges

1- Descriptif de l'existant

L'infrastructure existante repose sur un poste de travail fixe servant de support à l'environnement de virtualisation. Ce poste est équipé du logiciel VMware Workstation, permettant l'exécution de plusieurs machines virtuelles dans un cadre de travaux pratiques.

La connectivité réseau est assurée par une connexion Internet unique, fournie par le réseau hôte, à laquelle les machines virtuelles peuvent accéder via les mécanismes de virtualisation réseau proposés par VMware Workstation (interfaces virtuelles de type NAT ou pont).

Dans cette configuration, un pare-feu pfSense est déployé sous forme de machine virtuelle et joue le rôle de passerelle réseau. Il assure les fonctions de filtrage, de routage et de sécurisation des flux entre le réseau interne virtualisé et le réseau externe. L'ensemble des communications réseau dépend de ce pare-feu unique, qui constitue actuellement le point central de l'architecture.

L'architecture en place est de type non redondé. Aucune solution de haute disponibilité n'est implémentée, et il n'existe pas de mécanisme de bascule automatique en cas de défaillance du pare-feu. Une panne de la machine virtuelle pfSense, qu'elle soit liée à un incident logiciel, à un arrêt involontaire ou à un problème sur le poste hôte, entraînerait une interruption totale de l'accès réseau pour l'ensemble des machines virtuelles dépendantes.

De plus, les états de connexion ne sont pas conservés ni synchronisés, ce qui signifie qu'un redémarrage du pare-feu provoquerait la perte des sessions actives. L'infrastructure actuelle présente ainsi un point de défaillance unique, incompatible avec les exigences de continuité de service et de disponibilité attendues dans un contexte professionnel.

2- Besoins

Face aux limites de l'infrastructure existante, il apparaît nécessaire de mettre en place une solution permettant d'assurer la continuité de service réseau. Le besoin principal est d'éliminer le point de défaillance unique représenté par le pare-feu pfSense actuellement déployé sous forme de machine virtuelle unique.

L'infrastructure doit pouvoir tolérer la défaillance d'un pare-feu sans interruption perceptible pour les utilisateurs ou les machines virtuelles. Cela implique la mise en œuvre d'un mécanisme de haute disponibilité, capable d'assurer une bascule automatique vers un équipement de secours en cas d'incident.

Un autre besoin essentiel concerne la conservation des sessions réseau actives. En cas de bascule, les connexions en cours ne doivent pas être interrompues, ce qui nécessite la synchronisation des états de connexion entre les pare-feu. Cette exigence est particulièrement importante pour les services sensibles aux coupures, tels que les accès distants ou les applications réseau persistantes.

La solution retenue doit également permettre une administration centralisée et cohérente des règles de filtrage et des paramètres de sécurité, afin de garantir un comportement identique des deux pare-feu et de limiter les erreurs de configuration. Elle doit rester compatible avec l'environnement de virtualisation existant, basé sur VMware Workstation, et ne pas nécessiter de matériel supplémentaire dédié.

Enfin, le dispositif mis en place doit rester simple à déployer, à tester et à maintenir, dans un contexte pédagogique de travaux pratiques, tout en respectant les principes et les bonnes pratiques rencontrés en environnement professionnel.

3- Contraintes

La mise en œuvre de la solution de redondance s'inscrit dans un contexte de travaux pratiques, ce qui impose plusieurs contraintes d'ordre technique et organisationnel. L'ensemble de l'infrastructure doit être déployé sur un poste de travail fixe unique, sans ajout de matériel physique supplémentaire. Les ressources matérielles disponibles, notamment le processeur, la mémoire vive et l'espace de stockage, sont donc limitées à celles du poste hôte.

L'environnement de virtualisation utilisé est VMware Workstation, ce qui conditionne les possibilités de configuration réseau, notamment en ce qui concerne la gestion des interfaces virtuelles, des réseaux internes et des modes de connexion vers l'extérieur. La solution retenue doit être pleinement compatible avec cet outil et ne pas nécessiter de fonctionnalités avancées propres à des hyperviseurs de type serveur.

La connexion à Internet repose sur l'accès réseau du poste hôte. Il n'existe qu'un seul lien WAN, non redondé, ce qui signifie que la haute disponibilité ne peut s'appliquer qu'au niveau du pare-feu virtuel et non à la connectivité Internet elle-même. Cette contrainte limite la portée de la redondance à l'infrastructure logicielle.

Par ailleurs, les technologies mises en œuvre doivent rester gratuites ou incluses nativement dans pfSense, afin de respecter le cadre pédagogique et d'éviter toute contrainte liée à des licences logicielles.

Enfin, la solution doit être suffisamment stable et compréhensible pour permettre sa validation par des tests fonctionnels, tout en restant conforme aux bonnes pratiques professionnelles attendues dans le cadre du BTS SIO SISR.

II/ Ressources

1- Ressources mises à disposition

Dans le cadre de ce travail pratique, les ressources mises à disposition reposent sur un poste de travail fixe servant de support à l'ensemble de l'infrastructure. Ce poste est équipé du système d'exploitation hôte et dispose d'une connexion Internet fonctionnelle, utilisée pour fournir l'accès réseau aux machines virtuelles.

Le logiciel de virtualisation VMware Workstation est installé sur ce poste. Il permet la création, la configuration et l'exécution de plusieurs machines virtuelles simultanément, ainsi que la gestion des réseaux virtuels nécessaires à la mise en œuvre de l'architecture étudiée. Les fonctionnalités natives de VMware Workstation sont exploitées pour simuler les différents segments réseau, notamment le réseau WAN virtuel, le réseau LAN interne et le réseau dédié à la synchronisation des pare-feu.

Les images d'installation du pare-feu pfSense sont mises à disposition afin de déployer plusieurs instances identiques du système. Ces instances permettent la configuration d'un mécanisme de redondance basé sur les technologies CARP et pfsync, intégrées nativement à pfSense.

Une machine virtuelle sous Windows 10 est également disponible et utilisée en tant que poste client. Cette machine permet de générer du trafic réseau et de tester le bon fonctionnement de la haute disponibilité, notamment la continuité des connexions lors des scénarios de bascule entre les pares-feux.

Enfin, les supports pédagogiques associés au TP, tels que la documentation technique, complètent les ressources nécessaires à la réalisation de l'activité.

2- Ressource nécessaire à la mise en place

La mise en place de la solution de redondance nécessite, en premier lieu, la création et la configuration de plusieurs machines virtuelles au sein de VMware Workstation. Deux machines virtuelles distinctes sont requises pour héberger les pare-feu pfSense configurés en haute disponibilité, ainsi qu'une machine virtuelle supplémentaire sous Windows 10 utilisée comme poste client pour les tests.

Chaque machine virtuelle doit disposer de ressources matérielles adaptées, notamment en termes de mémoire vive, de capacité de stockage et d'interfaces réseau virtuelles. Les pare-feu pfSense nécessitent plusieurs cartes réseau virtuelles afin de séparer les flux WAN, LAN et de synchronisation, condition indispensable au bon fonctionnement de CARP et de pfsync.

La configuration de réseaux virtuels dédiés est également nécessaire. Un réseau WAN virtuel doit permettre l'accès à Internet via le poste hôte, un réseau LAN virtuel doit assurer la communication avec le poste client, et un réseau spécifique doit être réservé à la synchronisation des états et des configurations entre les pare-feu. Ces réseaux sont créés et gérés à l'aide des outils fournis par VMware Workstation.

Enfin, la mise en œuvre de la solution requiert l'accès à la documentation officielle de pfSense, notamment pour la configuration de la haute disponibilité, ainsi que le respect des bonnes pratiques de sécurité réseau. Ces éléments sont indispensables pour garantir une configuration fonctionnelle, stable et conforme aux objectifs du TP.

3- Gestion des ressources

La gestion des ressources dans ce TP repose sur une organisation optimisée des machines virtuelles et des réseaux virtuels au sein de VMware Workstation, afin de garantir la disponibilité et la stabilité de l'infrastructure.

Le poste hôte fixe est utilisé comme plateforme unique pour l'ensemble des VM. Les ressources matérielles du poste, telles que la mémoire vive, le processeur et le stockage, sont allouées de manière proportionnée à chaque machine virtuelle. Les pare-feu pfSense disposent ainsi de suffisamment de ressources pour exécuter leurs fonctions de filtrage, de routage et de synchronisation, tandis que la VM Windows 10 cliente reçoit une allocation adaptée pour réaliser des tests de continuité réseau sans affecter les performances globales.

Les réseaux virtuels sont configurés pour séparer clairement les flux WAN, LAN et la synchronisation entre les pares-feux, assurant ainsi l'isolation nécessaire et réduisant les risques de conflit ou de saturation. Chaque VM utilise des adresses IP fixes pour faciliter la configuration CARP et la surveillance des communications réseau.

La gestion des ressources comprend également la planification des tests, afin de limiter les conflits de trafic et de garantir que les bascules entre pare-feu peuvent être observées de manière contrôlée sur la machine cliente. Les sauvegardes régulières des configurations pfSense sont prévues pour permettre un retour rapide à un état fonctionnel en cas de problème lors des manipulations.

Ainsi, l'organisation et la gestion des ressources permettent de maintenir un environnement stable, fonctionnel et reproductible, conforme aux objectifs pédagogiques et aux bonnes pratiques de la haute disponibilité réseau.

III/ Analyse

1- Descriptifs des solutions

Trois solutions principales peuvent être envisagées pour améliorer la disponibilité et la continuité du service réseau.

La première solution est l'équilibrage de charge. Elle consiste à répartir le trafic réseau entre plusieurs pare-feu ou serveurs afin de réduire la charge sur chaque équipement et d'améliorer la performance globale. Chaque équipement traite une partie du trafic, ce qui peut permettre une meilleure répartition des ressources.

La deuxième solution est le failover. Dans ce mode, un pare-feu secondaire est configuré pour prendre le relais automatiquement en cas de défaillance du pare-feu principal. Cette méthode permet de basculer le trafic vers le pare-feu secondaire lorsque le principal devient indisponible.

La troisième solution est le basculement avec CARP et pfsync. CARP (Common Address Redundancy Protocol) permet de partager une adresse IP virtuelle entre plusieurs pares-feux, de sorte qu'un seul soit actif à la fois pour gérer le trafic réseau. pfsync permet la synchronisation des états de connexion et de la configuration entre les pares-feux, ce qui assure que les sessions en cours peuvent être conservées lors d'un basculement.

2- Comparaisons des solutions

Critères	Équilibrage de charge	Failover	Basculement CARP + pfsync
Principe	Répartit le trafic entre plusieurs pare-feu/serveurs	Un pare-feu secondaire prend le relais en cas de panne du principal	Adresse IP virtuelle partagée et synchronisation des états de connexion
Continuité des sessions	Non garantie	Non garantie	Oui
Bascule automatique	Partielle ou optionnelle	Oui	Oui
Gestion du trafic	Trafic réparti entre les équipements	Trafic basculé vers le secondaire	Trafic dirigé vers le pare-feu actif
Complexité de configuration	Moyenne à élevée	Faible à moyenne	Moyenne
Tolérance aux pannes matérielles	Limitée (les sessions peuvent être interrompues)	Permet de continuer le service en cas de panne du principal	Permet de continuer le service et conserve les sessions actives

3- Choix d'une solution

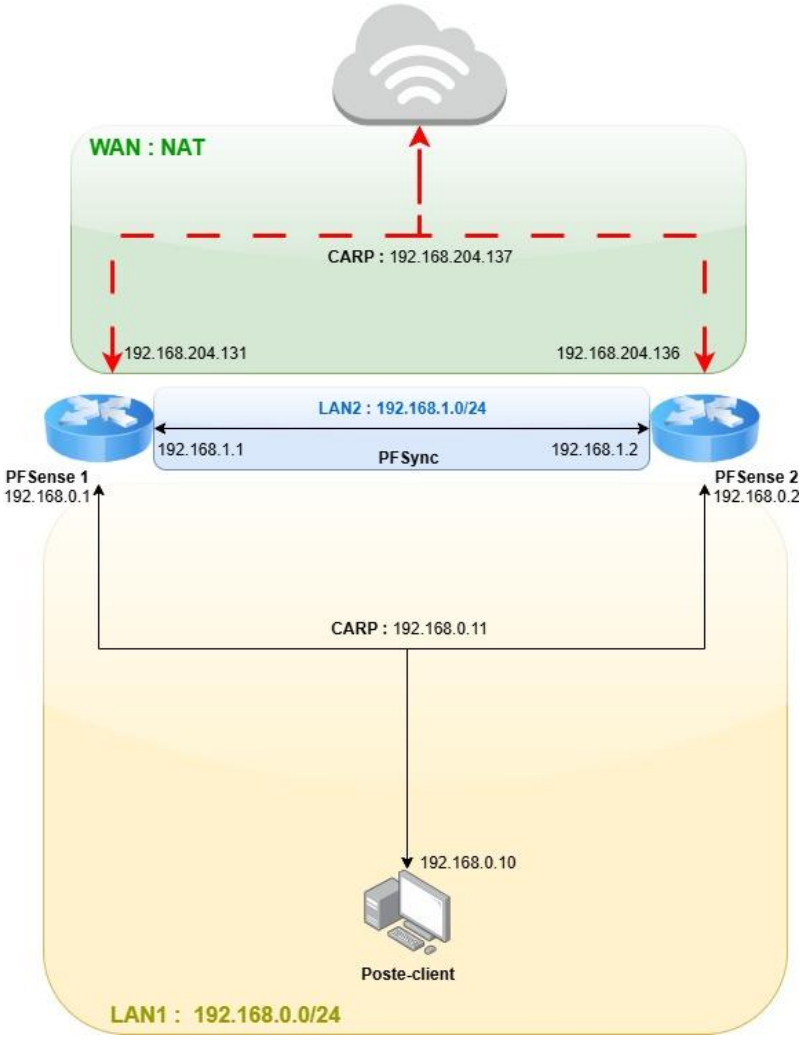
Après avoir analysé les différentes solutions de redondance disponibles, la solution retenue pour ce TP est le basculement avec CARP et pfsync. Ce choix est basé sur les besoins identifiés, notamment la nécessité d'assurer une continuité de service réseau et de maintenir les sessions actives lors d'une panne du pare-feu principal.

CARP permet de partager une adresse IP virtuelle entre plusieurs pares-feux, de sorte qu'un seul équipement soit actif pour gérer le trafic réseau à un instant donné. En parallèle, pfsync assure la synchronisation des états de connexion et de la configuration entre les pares-feux, permettant ainsi aux sessions existantes de continuer à fonctionner sans interruption lors du basculement.

Cette solution répond aux contraintes du TP : elle est compatible avec l'environnement de virtualisation VMware Workstation, exploite les fonctionnalités intégrées de pfSense, et peut être configurée et testée avec les ressources disponibles. Elle permet également d'illustrer de manière pratique le fonctionnement d'une infrastructure de haute disponibilité avec un double pare-feu dans un contexte pédagogique.

4- Cartographie du réseau

a) Schéma



b) Plan d'adressage

- **Réseau LAN1 : postes client :**

Équipement	Interface	Adresse IP
Adresse		192.168.0.0/24
Masque		255.255.255.0
Poste client	LAN	192.168.0.10
pfSense 1	LAN1	192.168.0.1
pfSense 2	LAN1	192.168.0.2
CARP LAN1	Virtuelle	192.168.0.11

- **Réseau LAN2 – Synchronisation pfsync :**

Équipement	Interface	Adresse IP
Réseau		192.168.1.0/24
Masque		255.255.255.0
pfSense 1	LAN2 (Sync)	192.168.1.1
pfSense 2	LAN2 (Sync)	192.168.1.2

- **Réseau WAN – Accès Internet (réseau virtuel VMware) :**

Équipement	Interface	Adresse IP
Réseau		192.168.204.0/24
Masque		255.255.255.0
pfSense 1	WAN	192.168.204.131
pfSense 2	WAN	192.168.204.136
CARP WAN	Virtuelle	192.168.204.137

c) Tables de routage

- **PFSense 1 :**

Destination	Masque	Passerelle	Interface
192.168.0.0	255.255.255.0	Directement connecté	192.168.0.1
192.168.1.0	255.255.255.0	Directement connecté	192.168.1.1
192.168.204.0	255.255.255.0	Directement connecté	192.168.204.131
0.0.0.0	0.0.0.0	Passerelle WAN	192.168.204.131

- **PFSense 2 :**

Destination	Masque	Passerelle	Interface
192.168.0.0	255.255.255.0	Directement connecté	192.168.0.2
192.168.1.0	255.255.255.0	Directement connecté	192.168.1.2
192.168.204.0	255.255.255.0	Directement connecté	192.168.204.136
0.0.0.0	0.0.0.0	Passerelle WAN	192.168.204.136

5- Etude de l'impact sur le SI existant

a) Sécurité

La mise en place de deux pare-feu pfSense redondés avec CARP et pfsync renforce la sécurité globale du système d'information en supprimant le point de défaillance unique lié à un pare-feu isolé. En cas de panne, le basculement automatique permet de maintenir les fonctions de filtrage et de protection du réseau.

La synchronisation des configurations et des états de connexion garantit une cohérence des règles de sécurité entre les deux pares-feux, évitant toute divergence lors d'un changement de rôle. L'utilisation d'un réseau dédié à la synchronisation pfsync permet d'isoler ces échanges sensibles du reste du réseau.

Cette architecture implique toutefois une gestion rigoureuse des accès administratifs et des interfaces de synchronisation afin d'éviter toute exposition inutile. Dans ce contexte, l'impact sur la sécurité du système d'information est globalement positif.

b) Performance

La mise en place d'une architecture de redondance avec deux pare-feu pfSense entraîne un impact limité sur les performances du système d'information. En fonctionnement normal, un seul pare-feu traite le trafic réseau, tandis que le second reste en attente, ce qui ne modifie pas le cheminement des flux par rapport à l'architecture initiale.

La synchronisation des états de connexion via pfsync génère un trafic supplémentaire, mais celui-ci reste faible et est isolé sur un réseau dédié. Ce trafic n'a donc pas d'impact significatif sur les performances du réseau LAN ou WAN.

L'utilisation de machines virtuelles sur un même poste hôte implique un partage des ressources matérielles. Une allocation adaptée de la mémoire et du processeur permet de limiter les risques de dégradation des performances, tant pour les pares-feux que pour le poste client.

Dans l'ensemble, l'architecture de redondance n'entraîne pas de baisse notable des performances, à condition que les ressources du poste hôte soient correctement dimensionnées.

6- Phasage de l'intervention

L'intervention est découpée en plusieurs phases successives afin de garantir une mise en œuvre structurée et maîtrisée de la solution de redondance.

La première phase consiste à préparer l'environnement de travail. Elle comprend la vérification des ressources disponibles sur le poste hôte, la création des réseaux virtuels nécessaires dans VMware Workstation et le déploiement des machines virtuelles pfSense et Windows 10.

La deuxième phase est dédiée à la configuration initiale des pare-feu pfSense. Les interfaces réseau (WAN, LAN1 et LAN2 dédié à pfsync) sont configurées avec les adresses IP prévues, ainsi que les règles de filtrage de base permettant la communication entre les différents réseaux.

La troisième phase porte sur la mise en place de la haute disponibilité. Elle inclut la configuration des adresses IP virtuelles CARP sur les interfaces WAN et LAN, l'activation et le paramétrage de la synchronisation pfsync, ainsi que la synchronisation des configurations via XMLRPC.

La quatrième phase consiste à réaliser les tests de fonctionnement. Des scénarios de coupure et de basculement sont effectués afin de vérifier la continuité de service et le maintien des sessions depuis le poste client.

7- Prévision des tests de validation

Les tests de validation prévus pour cette intervention sont les suivants :

- **Test de connectivité réseau**
  Vérification de l'accès au réseau externe depuis le poste client en utilisant l'adresse IP virtuelle CARP du LAN comme passerelle par défaut.
- **Test du fonctionnement de CARP**
  Contrôle de l'état actif/passif des pare-feu afin de s'assurer que le pare-feu maître gère le trafic en situation normale.
- **Test de synchronisation des configurations**
  Modification d'un paramètre ou d'une règle de filtrage sur le pare-feu maître, puis vérification de sa réplication automatique sur le pare-feu esclave via XMLRPC.
- **Test de synchronisation des états de connexion (pfsync)**
  Maintien d'une communication active depuis le poste client lors d'une simulation de basculement afin de vérifier la persistance des sessions.
- **Test de basculement (failover)**
  Arrêt volontaire du pare-feu maître ou désactivation d'une interface critique pour vérifier le passage automatique du rôle actif vers le pare-feu esclave.

Les résultats attendus sont la continuité de service, la cohérence des configurations entre les pares-feux et le maintien des connexions actives lors des scénarios de panne.

IV/ Mise en place

1- Réalisation

a) Mise en place des VMs

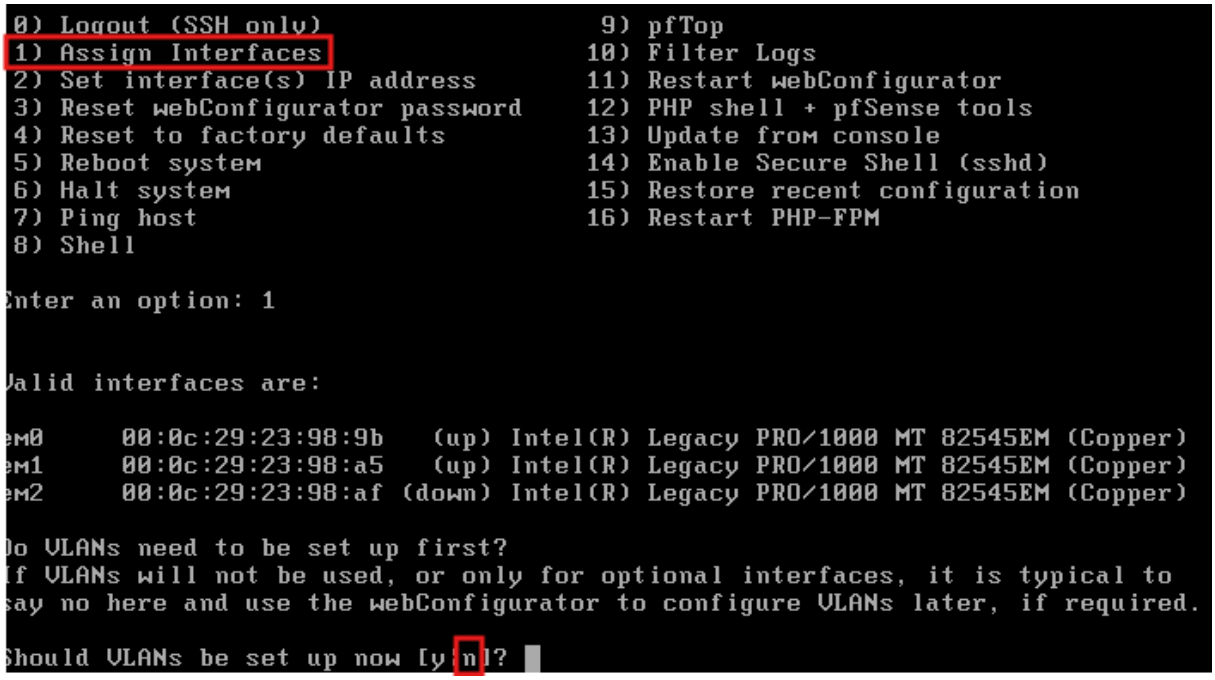
- **Installation des deux VMs PFSense :**
  - Mémoire : 256 Mo
  - Processeur : 1
  - Disque dur : 10 Go
  - 3 interfaces réseaux dont un en NAT

  Installation : Installation et configuration de PFSense

Dans cette procédure, il ne sera pas nécessaire de suivre les règles de pare-feu et la table de routage qui y sont proposés. Nous nous occuperons de ces paramètres dans un second temps.

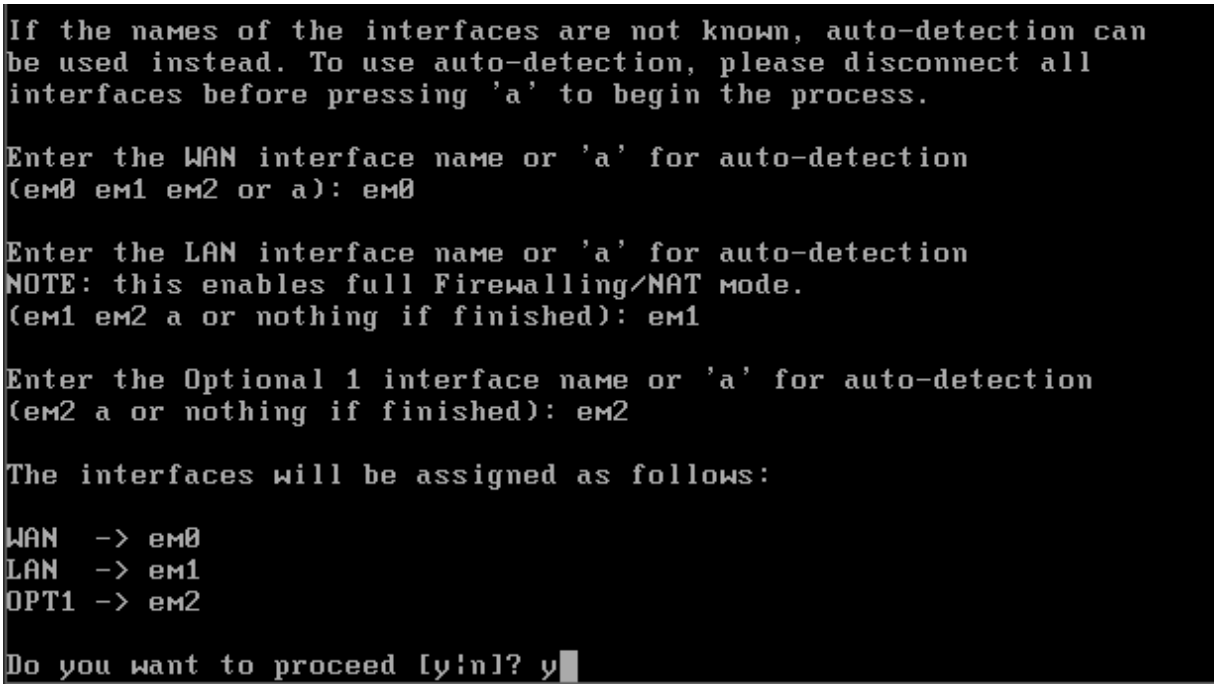
Une fois la troisième interface ajoutée « physiquement » sur le pare feu, nous allons la rajouter :

Une fois PFSense lancé choisir 1 pour assigner une interface puis répondre non lorsque l'on vous demande de choisir un VLAN.



Choisir le nom à attribuer pour chaque interface :

- WAN : em0
- LAN : em1
- OPT1 : em2



Je pourrais ensuite lui attribuer l'adresse IP correspondante.

- **Installation du poste client :**
    - Mémoire 4 Go
    - Processeur : 2
    - Disque dur : 40 Go

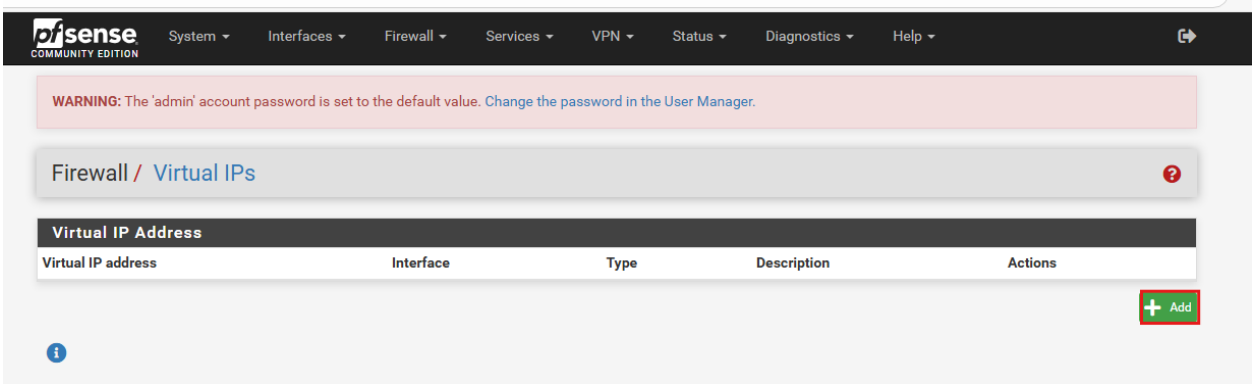
  Installation : Installation d'un poste sous Windows 10

b) Mise en place de CARP sur les pare-feux

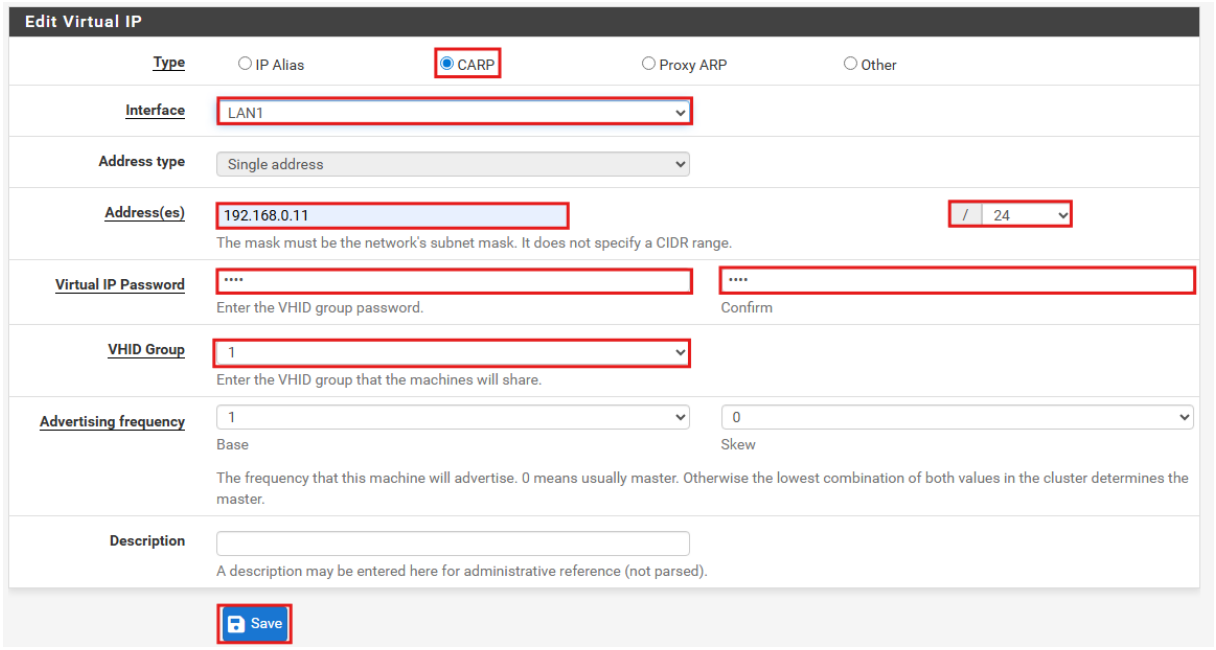
Je vais maintenant configurer CARP entre les interfaces LAN1 des deux pares-feux et entre les interfaces WAN de ces mêmes pares-feux, afin de créer une interface virtuelle qui servira de passerelle.

Cette configuration est à réaliser sur les deux pares-feux :

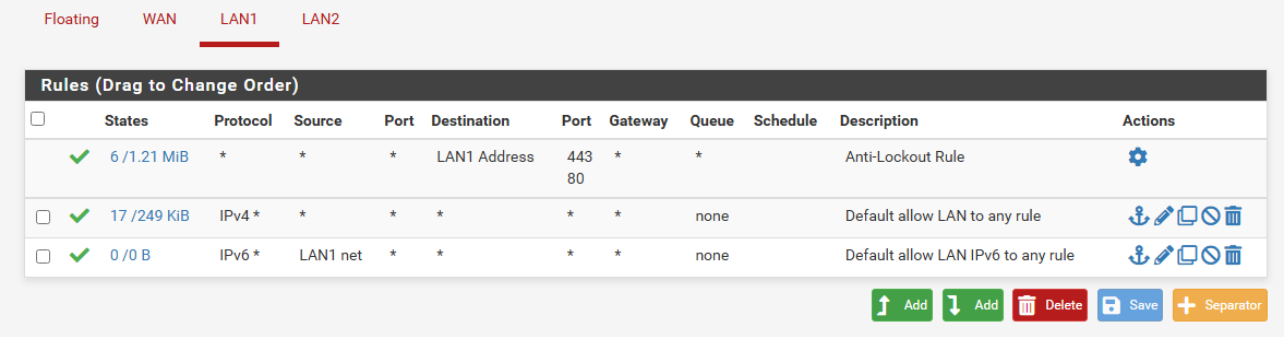
- Aller dans Firewall / Virtual IPs puis ajouter une adresse virtuelle



- Sélectionner l'interface LAN1 et renseigner les informations comme ci-dessous :
    - Choisir CARP
    - Renseigner l'interface LAN1
    - Indiquer l'adresse IP virtuelle de cette interface
    - Renseigner le mot de passe
    - Choisir un ID de groupe



- Renseigner les mêmes informations sur le PFSense2 et refaire la même chose pour l'interface WAN.
- Une fois l'interface virtuelle créer pour le LAN1, je vais pouvoir l'indiquer comme passerelle sur mon poste client. Je vais ainsi pouvoir naviguer d'un pare-feu à un autre via un navigateur web sans changer la passerelle.
- Aller dans Firewall / Rules et configurer les règles de pare-feu comme ci-dessous :

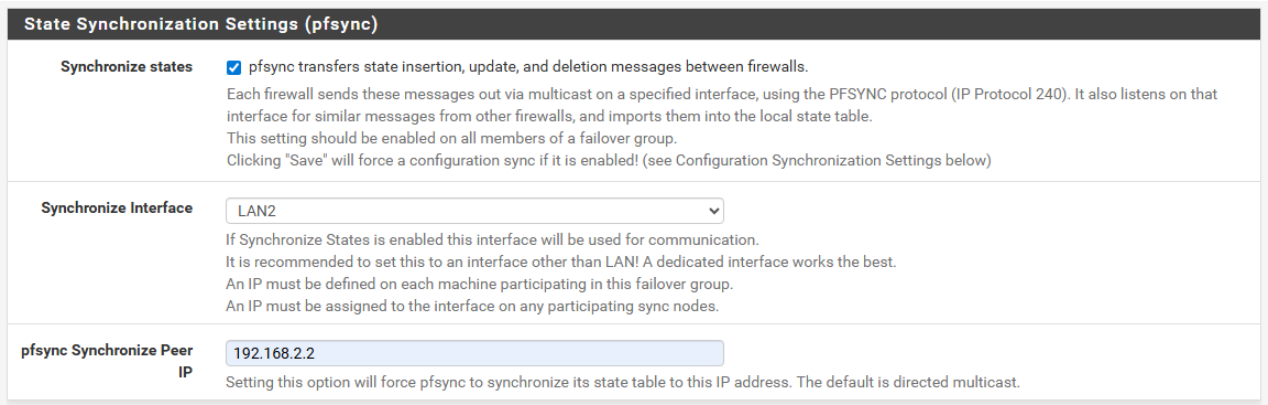


c) Mise en place de la haute disponibilité

Je vais désormais configurer le lien PFSync qui me permettra de synchroniser mon pare-feu maître avec mon pare-feu esclave. Grâce à ça, chaque modification du pare-feu maître se répercutera sur le pare-feu esclave.

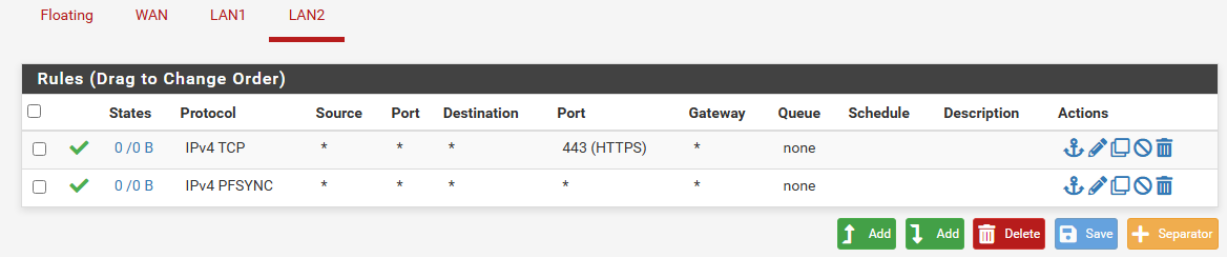
Dans PFSense1 :

- Aller dans System / High Availability Sync et cocher pfsync transfers state insertion
- Synchronize Interface : LAN2
- Pfsync synchronizer peer IP : indiquer l'adresse ip de l'interface LAN2 du second pare-feu



- Synchronize config to ip : indiquer la même adresse que précédemment
- Remote system username et Remote system password : renseigner vos login admin pour se connecter à pfsense
- Enfin sélectionner toutes les options de Select option to sync

- Aller ensuite dans Firewall / Rules et configurer les règles de pare-feu comme ci-dessous :



Dans PFSense2 :

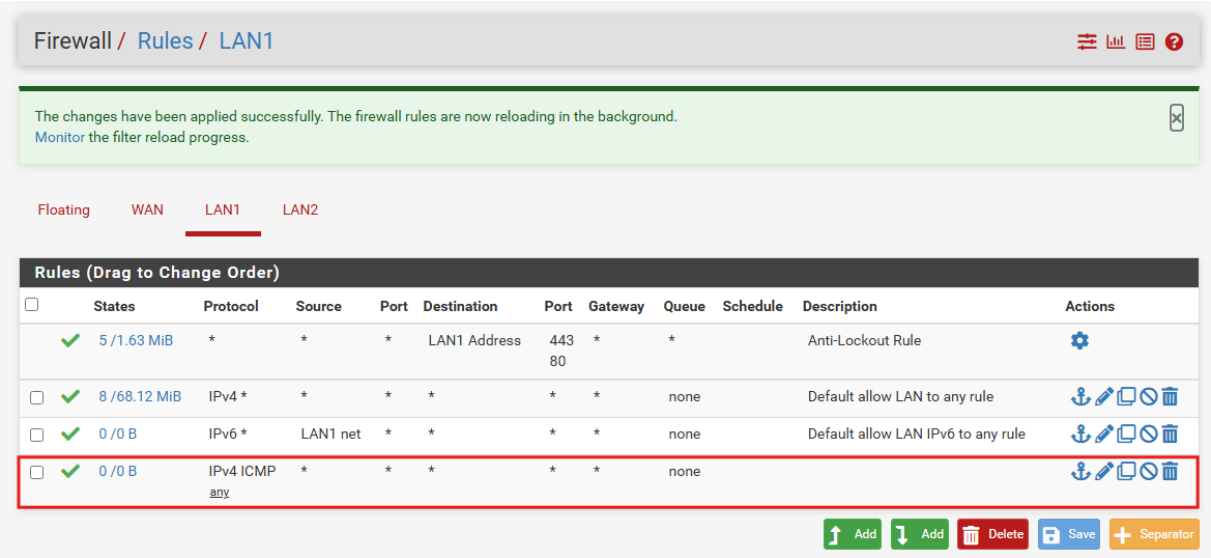
- Aller dans System / High Availability Sync et configurer de la même manière que pour PFSense1. Cependant ne pas remplir la partie XMLRPC Sync.
- Du côté règle de pare-feu, dans LAN2, ajouter les mêmes règles que pour PFSense1.

2- Rapport de tests

a) Synchronisation des Pares-feux

Pour tester la synchronisation entre les pares-feux, je vais ajouter une règle de pare-feu sur le pare-feu maître. Celle-ci devra se répliquer sur le pare-feu esclave.

Je vais par exemple ajouter l'autorisation d'utiliser le port ICMP sur le LAN1



En allant sur PFSense2 je peux m'apercevoir que cette règle c'est bien répliqué.

b) Haute disponibilité

Pour vérifier que le pare-feu esclave prend le relais en cas de panne du pare-feu maître, je vais simuler une panne sur ce dernier en l'éteignant. Je vais ensuite faire un ping sur le web depuis mon poste client afin de vérifier que le pare-feu esclave à bien pris le relais. Si cela fonctionne alors la redondance du pare-feu est opérationnelle.

3- Rapport de déploiement

Le déploiement de la solution de redondance des pare-feu pfSense a été réalisé conformément au phasage défini lors de la phase d'analyse. L'ensemble des machines virtuelles a été déployé sur un poste

hôte équipé de VMware Workstation, en utilisant des réseaux virtuels distincts pour le WAN, le LAN utilisateur et la synchronisation pfsync.

Les deux pare-feu pfSense ont été configurés avec les adresses IP prévues sur leurs interfaces respectives. Les adresses IP virtuelles CARP ont été mises en place sur les interfaces WAN et LAN afin d'assurer une passerelle unique pour le réseau interne et un point d'accès unique vers l'extérieur.

La synchronisation des configurations via XMLRPC ainsi que la synchronisation des états de connexion via pfsync ont été activées et vérifiées. Les règles de filtrage et les paramètres réseau ont été correctement répliqués entre le pare-feu maître et le pare-feu esclave.

Les tests de basculement ont confirmé le bon fonctionnement de la haute disponibilité. Lors de l'arrêt du pare-feu maître, le pare-feu esclave a pris automatiquement le relais sans perte de connectivité pour le poste client. Les communications actives ont été maintenues, validant la synchronisation des états.

Le déploiement peut être considéré comme fonctionnel et conforme aux objectifs fixés, assurant la continuité de service et la cohérence des configurations dans un contexte de redondance de pare-feu.

V/ Bilan

1- Conclusion

Ce TP a permis de mettre en œuvre une solution de redondance de pare-feu basée sur deux machines virtuelles pfSense utilisant les technologies CARP et pfsync. L'architecture déployée répond aux objectifs de continuité de service et de haute disponibilité en supprimant le point de défaillance unique lié à un pare-feu isolé.

Les tests réalisés ont confirmé le bon fonctionnement du basculement automatique ainsi que la synchronisation des configurations et des états de connexion entre les pares-feux. L'accès réseau du poste client a été maintenu lors des scénarios de panne, validant l'efficacité de la solution mise en place.

Cette expérimentation a permis d'aborder des notions essentielles liées à la haute disponibilité des équipements de sécurité, tout en mettant en évidence l'importance d'une configuration rigoureuse et d'une bonne organisation des réseaux. La solution déployée constitue une base fiable et reproductible pour des environnements nécessitant une disponibilité accrue des services réseau.

2- Auto-évaluation

La réalisation de ce TP a permis de mobiliser et de renforcer plusieurs compétences techniques liées aux réseaux et à la sécurité. La configuration des pare-feu pfSense, la mise en place de la redondance avec CARP et la synchronisation des états via pfsync ont été menées à bien conformément aux objectifs fixés.

La compréhension des mécanismes de haute disponibilité, ainsi que la gestion des interfaces réseau et des adresses IP virtuelles, ont été correctement assimilées. Les tests de basculement et de synchronisation ont permis de valider la solution et d'identifier l'importance d'une configuration rigoureuse, notamment en matière de règles de filtrage et de réseaux dédiés.

Ce TP a également permis de développer une méthodologie de travail structurée, allant de l'analyse des besoins à la validation du déploiement. Des difficultés mineures ont été rencontrées lors de la configuration initiale, mais elles ont été résolues par l'analyse et la vérification des paramètres, contribuant ainsi à l'apprentissage.

Dans l'ensemble, les objectifs pédagogiques du TP sont atteints et les compétences acquises pourront être réinvesties dans des contextes professionnels nécessitant des solutions de haute disponibilité et de sécurisation des infrastructures réseau.