Mise en place de la haute disponibilité pour les pares-feux PfSense

Hachet Nicolas BTS SIO 2025

Sommaire :

Environnement technique :

Voici ci-dessous la fiche de l'environnement technique de la maquette.

Environement Technique pour les deux dossiers E5		
Qui	**Quoi**	**Solution ?**
Mise à disposition par le centre de formation	Gestion des incidents	Jira
	Détection et prévention des intrusions	WAZUH
	Chiffrement	Bitlocker
	Analyse de trafic	PFSENSE
Maquette à créer par l'apprenant dans la globalité	Un réseau comportant plusieurs périmètres de sécurité	Sous-réseau Pfsense et fortinate, Vlan sur Switch CISCO
	Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	GLPI
	Un logiciel d'analyse de trames	Wireshark
	Un logiciel de gestion des configurations	Glpi + Fusion Inventory
	Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	VPN
	Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	WAZUH
	Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Pfsense + fortigate
	Une solution garantissant la continuité d'un service	SSH, VPN
	Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Raid, Onduleurs
	Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HAPROXY
Une option à choisir par l'apprenant et à intégrer dans sa maquette	Une solution permettant la connexion sécurisée entre deux sites distants	VPN inter-sites
	Une solution permettant le déploiement des solutions techniques d'accès	FOG
	Une solution gérée à l'aide de procédures automatisées écrites avec un langage de scripting	Powerschell
	Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Pfsense

Description du projet :

Vous trouverez sur les deux pages suivantes la description de la réalisation professionnelle de mon premier projet proposé. Je vous détaillerai tous les besoins nécessaires pour mener à bien la réalisation de ce projet.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

N° réalisation : 1

Nom, prénom : HACHET Nicolas

N° candidat : 02203360653

Épreuve ponctuelle [X] **Contrôle en cours de formation** [ ] **Date :** 13 / 03 / 2025

Organisation support de la réalisation professionnelle

Dans cette situation professionnelle, l'entreprise Dualya fait appel à nos services pour mettre en place la redondance des Pares-feux.

Intitulé de la réalisation professionnelle

J'ai donc installé deux machine virtuelle (deux Pares-feux), sur laquelle j'ai configuré la haute disponibilité et des adresse IP virtuelle.

Période de réalisation : Du 03/03/2025 au 07/03/2025 **Lieu :** CFA Fab'Academy - La Roche Sur Yon

Modalité : [X] **Seul(e)** [ ] **En équipe**

Compétences travaillées

- [X] Concevoir une solution d'infrastructure réseau
- [X] Installer, tester et déployer une solution d'infrastructure réseau
- [X] Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Ressources fournies : Un accès internet, un hyperviseur (machine virtuelles : deux Pares-feux, Windows 10), un ordinateur portable sous Windows 10

Ressources attendus : Une infrastructure fonctionnelle répondant à la demande du client avec deux Pares-feux virtialisé.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources documentaires : documentation technique, schéma réseau de l'entreprise Dualya.

Ressources matérielles : un hyperviseur avec des machines virtuelles configurées (Pare-feu, Windows 10) et un ordinateur portable avec Windows 10 installé.

Ressources logicielles : Draw.io, Mozilla Firefox, VMware, Windows 10, Haute disponibilité, IP Virtuel.

Modalités d'accès aux productions[3] et à leur documentation[4]

Tous les dossiers techniques et le guide des utilisateurs sont accessibles à l'adresse suivante : https://nicolas.hachet.formation-esiac.fr/

---

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

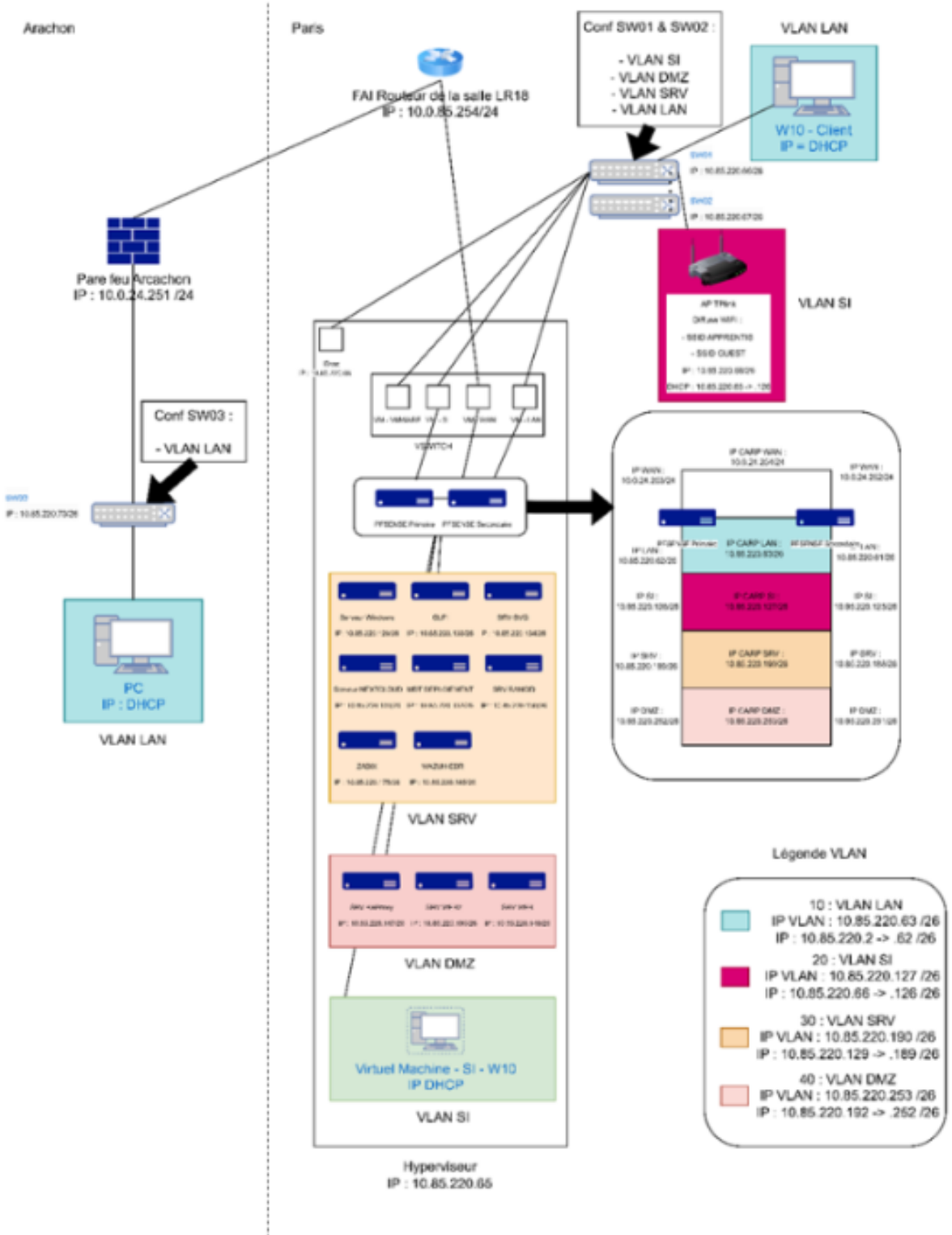
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Voici le schéma d'infrastructure respectant le schéma réseau, composée des deux Pares-feux installé sur des machines virtuelle.



Contexte :

L'entreprise Dualya, spécialisée dans l'art et la rénovation, connaît une expansion rapide, rendant essentiels les services mis à disposition de ses clients et employés. Afin de garantir un accès fiable et sécurisé à ses services, elle a fait appel au prestataire informatique HAssistance.

Dualya souhaite mettre en place une haute disponibilité des pares-feux afin d'éviter toute interruption de production en cas de perte de connexion.

Dans ce contexte, une problématique s'impose : comment assurer la haute disponibilité des pares-feux afin de garantir la continuité des services et prévenir toute interruption de production en cas de défaillance réseau ?

Choix de la solution :

Pour choisir la solution la plus adapté a l'entreprise Dualya nous avons fait un tableau comparatif, comparant 4 pares-feux soit 2 virtuels (PfSense et OPNsense) et 2 physiques (Fortinet et Stormshield).

Critère	**PfSense (virtuel)**	**OPNsense (virtuel)**	**Fortinet (physique)**	**Stormshield (physique)**
Coût	Gratuit / Open-source	Gratuit / Open-source	Élevé (matériel + licences)	Élevé (matériel + licences)
Licence	Aucune obligatoire	Aucune obligatoire	Licence FortiGuard obligatoire	Licence Stormshield obligatoire
Déploiement	Virtuel (Proxmox, VMware…)	Virtuel (Proxmox, VMware…)	Appliance matérielle	Appliance matérielle
Simplicité d'utilisation	Interface claire, stable	Interface moderne, intuitive	Interface propre à FortiOS	Interface Stormshield (plus technique)

Nous avons choisi, pour l'entreprise Dualya, d'utiliser des pares-feux PfSense virtuels, car ils sont gratuits et open source, ce qui représente une solution économique. De plus, PfSense étant une solution virtuelle, cela permet à Dualya de ne pas ajouter d'équipement physique supplémentaire.

Topologie physique :

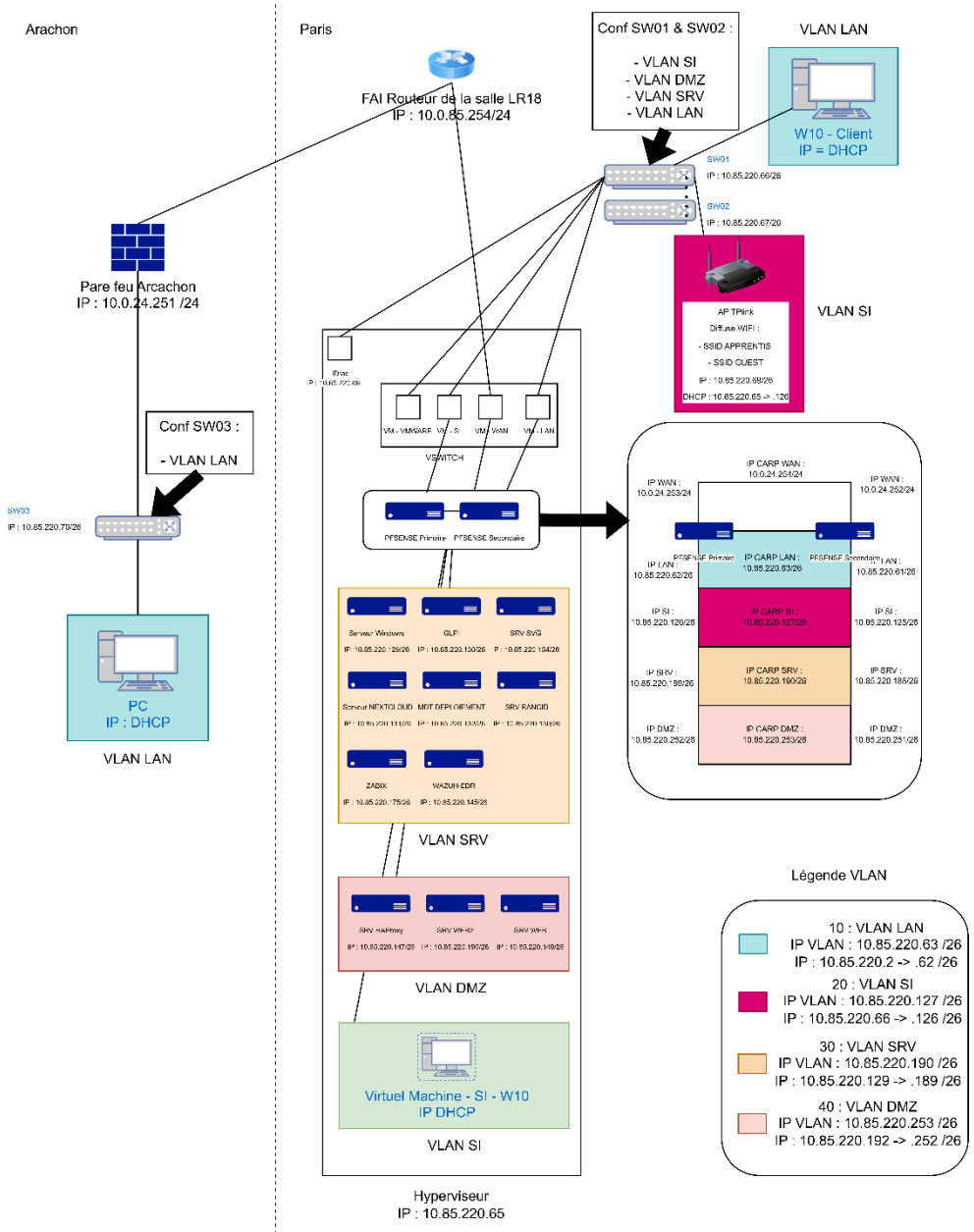


Schéma disponible dans l'annexe 1.

La maquette est basée sur l'architecture suivante et elle permet ainsi de garantir la connectivité, la sécurité et la haute disponibilité des pares-feux. Le réseau est segmenté en plusieurs VLANs afin d'assurer une isolation logique entre les différents services et contrôler les flux de données qui circulent. Un pare-feu physique (Fortinet) pour le site d'Arcachon et deux pares-feux logiques (PfSense) pour le site de Paris assurent la protection du système et le filtrage des accès au réseau. Il y a un serveur DHCP qui est utilisé pour attribuer dynamiquement des adresses IP aux différents équipements du réseau et un serveur AD dédié à la gestion des utilisateurs. De plus, un conteneur Keepass Web, accessible depuis le réseau de la salle BTS, permet d'accéder aux identifiants nécessaires à la connexion sur les machines.

Présentation des notions techniques :

Présentation du Pare-feu :

Un pare-feu est un dispositif de sécurité informatique qui surveille et contrôle le trafic réseau entrant et sortant d'un système. Il agit comme une barrière pour bloquer les accès non autorisés tout en permettant les connexions légitimes. Il peut être matériel ou logiciel. Son rôle principal est de protéger les réseaux contre les attaques externes et de filtrer les données malveillantes.

Présentation de la Haute Disponibilité :

La HA (High Availability), ou Haute Disponibilité, est un concept permettant d'assurer la continuité de service en évitant toute interruption due à une panne matérielle ou logicielle.

Dans le cas de PfSense, la HA est mise en place en utilisant un cluster de pare-feu redondants (un pare-feu principal et un pare-feu secondaire). Si le pare-feu principal tombe en panne, le secondaire prend automatiquement le relais grâce à CARP (Common Address Redundancy Protocol) et PFSync.

Présentation du protocole Carp :

Le CARP (Common Address Redundancy Protocol) est un protocole de redondance réseau qui fonctionne principalement au niveau de la couche réseau du modèle OSI et du modèle TCP/IP. Il permet d'assurer la haute disponibilité (HA) des équipements réseau, notamment des pare-feu PfSense. Grâce à la création d'adresses IP virtuelles partagées entre ces 2 pares-feux, il garantit un basculement automatique en cas de panne, assurant ainsi la continuité du service.

Convention de nommage :

Nous avons décidé d'utiliser une convention de nommage pour optimiser l'infrastructure de Dualya.

Une convention de nommage dans une infrastructure informatique, c'est un ensemble de règles définies pour nommer de manière cohérente les éléments techniques d'un système.

Machines :

EX : VM-FW-PA-01

VM -> Machine virtuelle

FW -> Nom de l'équipement (Firewall / Pare-feu)

PA -> Sites sur laquelle la machine se trouve (PA = Paris, AR = Arcachon)

01 -> Numéro de la machine en fonction de ses pairs, s'il y a deux Pares-Feux le deuxième serait le -02

Utilisateur :

Les machines seront administrées par l'utilisateur admin (administrateur) et un mot de passe.

Machines \ Compte	Identifiant	Mot de passe
VM-FW-PA-01	admin	(Keepass)
VM-FW-PA-02	admin	(keepass)

Configuration :

Plan d'adressage :

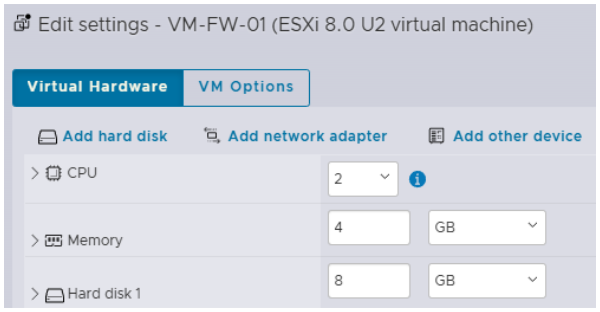
Services / Machines	VM-FW-01	VM-FW-02	CARP
WAN	10.0.24.253/24	10.0.24.252/24	10.0.85.200/24
LAN	X	X	X
VM_SRV	10.85.220.189/26	10.85.220.188/26	10.85.220.190/26
VM_SI	10.85.220.125/26	10.85.220.124/26	10.85.220.126/26
VM_LAN	10.85.220.61/26	10.85.220.60/26	10.85.220.62/26
VM_DMZ	10.85.220.253/26	10.85.220.252/26	10.85.220.254/26
SYNC	192.168.1.1/24	192.168.1.2/24	X

Le plan d'adressage a été conçu de manière que l'adresse IP virtuelle (CARP) de chaque réseau soit la dernière adresse IP utilisable. Une exception est faite pour l'adresse IP virtuelle (CARP) de l'interface WAN, qui doit appartenir au même sous-réseau que la passerelle pour fonctionner correctement.

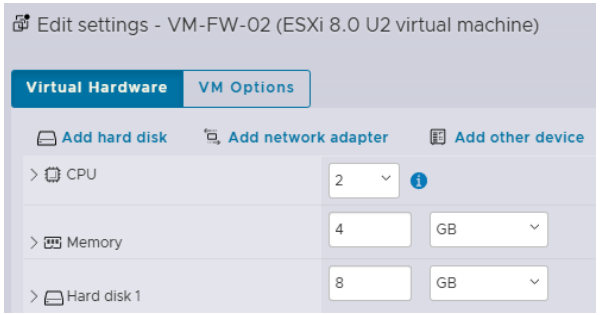
Physique :

Les pares-feux possèdent 2 processeurs, 4 Go de mémoire vive et 8 Go d'espace de stockage chacun. Cette configuration choisie permet à la machine d'être rapide et efficace lors de sa configuration.

Pares-feux 1 :



Pares-feux 2 :



Logiciel :

La configuration des deux Pares-feux est pratiquement identique puisque le but du HA est de faire une réplication néanmoins les adresses IP des 2 pares-feux sont quand même différés pour éviter les usurpations d'adresse IP.

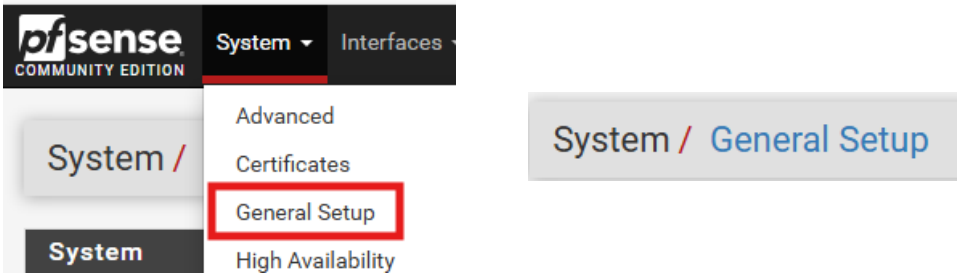
Préparation des pares-feux :

Pour commencer, nous avons installé le deuxième pare-feu. Ensuite, nous avons vérifié que les deux pares-feux étaient bien à l'heure, à jour et qu'ils avaient un accès à Internet.
Ces vérifications sont indispensables : en effet, si les pares-feux ne disposent pas de la même heure système ou s'ils ne sont pas dans la même version logicielle, la synchronisation ne pourra pas s'effectuer correctement.
Par ailleurs, la vérification de l'accès à Internet est également cruciale : en cas de perte de lien sur le pare-feu maître, le pare-feu de secours devra disposer d'un accès à Internet pour prendre le relais correctement.

Vérification de l'heure sur les pares-feux :

Pour vérifier que le pare-feu était à l'heure, nous nous sommes rendus sur la page principale de l'interface d'administration et avons consulté la section « Current date/time ».

Nous avons comparé cette heure avec celle de notre poste de travail, qui était correctement synchronisé, et avons constaté un décalage d'une heure.
Pour corriger cela, nous nous sommes rendus dans le menu « System », puis dans l'onglet « General Setup ».

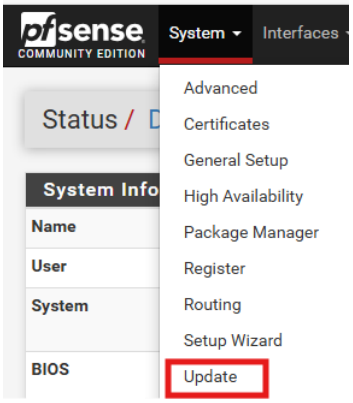


Ensuite, nous avons accédé à l'onglet « Localization », puis à la section « Timezone », où nous avons sélectionné « Europe/Paris ».
Après avoir redémarré le pare-feu, celui-ci a adopté la bonne heure.

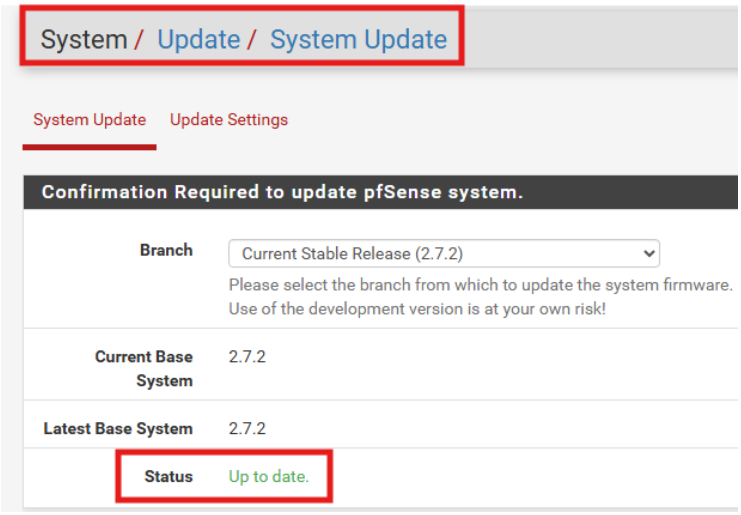
La même opération a été effectuée sur le pare-feu secondaire afin de garantir une parfaite synchronisation entre les deux équipements.

Vérification que le système est à jour :

Pour vérifier si le pare-feu était à jour, nous nous sommes rendus dans le menu « System », puis dans la section « Update ».
Cela nous a permis de consulter la version actuelle du système et de voir si des mises à jour étaient disponibles.



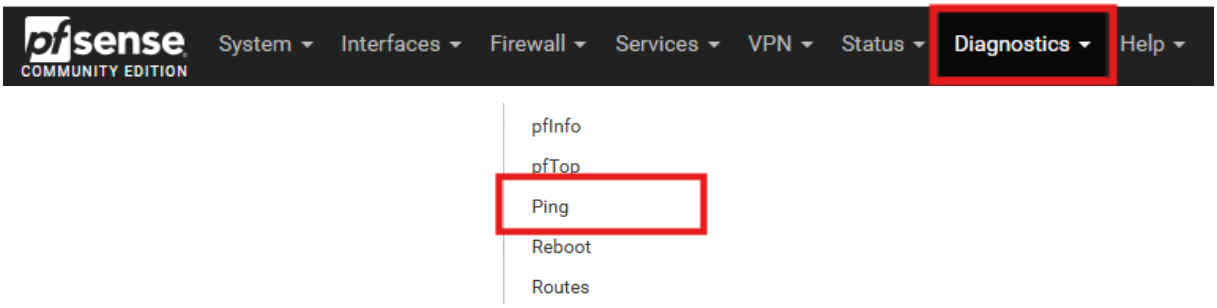
Si, sur la page « System Update », la ligne « Status » affiche « Up to date », cela signifie que le système est à jour.



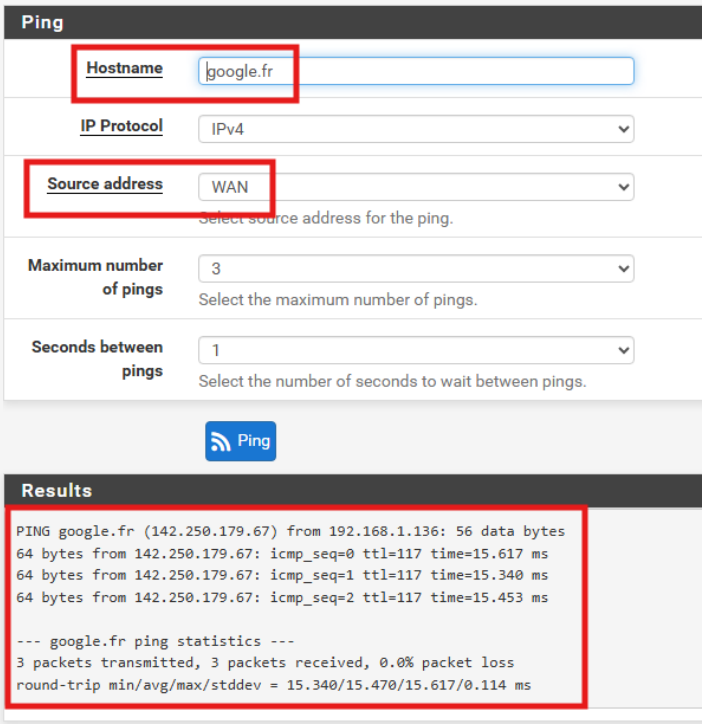
Le pare-feu principal étant à jour, nous avons effectué les mêmes vérifications et manipulations sur le pare-feu secondaire (Backup) afin de garantir qu'il était à jour.

Vérification de l'accès internet :

Pour finir, nous avons vérifié si les pares-feux avaient bien accès à Internet.
Pour cela, nous nous sommes rendus dans le menu « Diagnostics », puis dans la section « Ping ».



Nous avons ensuite effectué un test de ping depuis notre interface « WAN » vers « google.fr », ce qui nous a permis de vérifier que la communication avec Internet fonctionnait correctement et que la résolution DNS se faisait comme prévu.



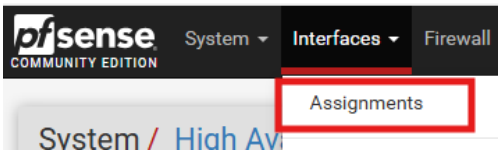
Le résultat du ping montrait que trois paquets avaient été envoyés et trois avaient été reçus, ce qui confirmait que la communication avec Internet était établie et que la résolution DNS fonctionnait correctement.
Nous avons ensuite répété cette manipulation sur le pare-feu Backup.
Après ces vérifications, les pares-feux étaient prêts pour la mise en place du HA.

Mise en place du HA sur le pare-feu Master :

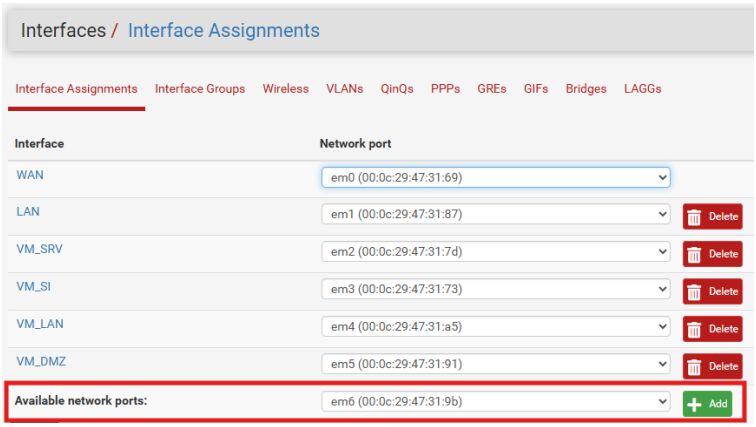
Création de l'interface de synchronisation :

Pour mettre en place le HA sur les pares-feux, il est nécessaire de dédier une interface exclusivement à la synchronisation, afin de permettre la communication entre les deux pares-feux sans surcharger les autres interfaces.
Nous avons donc créé une interface, que nous avons nommée « Sync », sur les deux pares-feux.
Pour cela, nous avons éteint les deux pares-feux, puis, dans l'interface d'ESXi, nous avons sélectionné « Edit », puis « Add network adapter », et avons attribué les deux nouvelles interfaces à un réseau isolé que nous avons nommé « Carp ».

Ensuite, nous avons redémarré les deux pares-feux et sommes retournés sur l'interface web pour configurer les deux nouvelles interfaces.
Pour les configurer, il fallait d'abord les ajouter. Nous sommes donc allés dans le menu « Interfaces », puis dans « Assignements ».



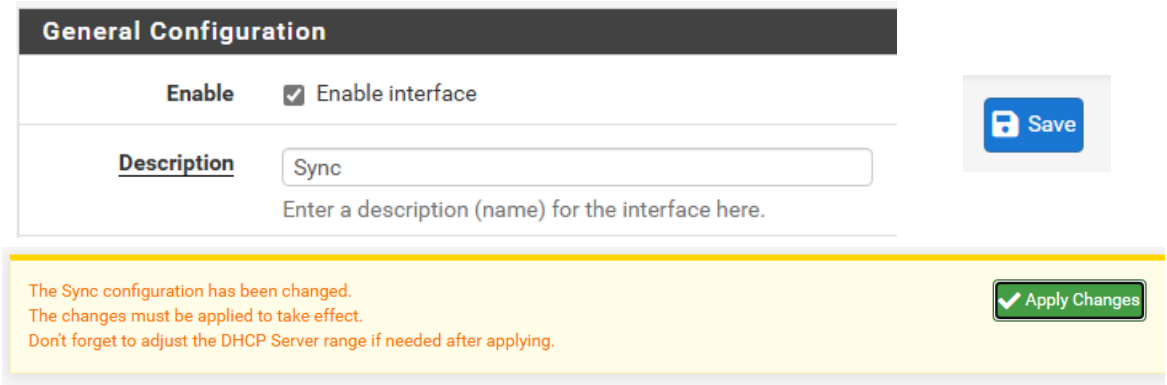
Sur la page « Assignments », tout en bas, nous avons trouvé une nouvelle carte réseau que nous avons pu ajouter (Add).



En cliquant sur « Add », la carte réseau a été ajoutée avec un nom (OPT suivi du numéro de la carte). Ensuite, en retournant dans « Interfaces », nous avons constaté que la nouvelle carte était bien présente.
Nous avons répété cette manipulation sur le pare-feu Backup.

Configuration de l'interface de synchronisation :

Pour configurer l'interface de synchronisation, nous sommes allés dans « Interfaces » et avons sélectionné OPT 5.
Nous avons commencé par cocher la case « Enable interface » pour activer l'interface, puis avons modifié la description pour qu'elle corresponde au nom de la carte, en saisissant « Sync ».
Ensuite, nous sommes allés en bas de la page pour enregistrer les modifications en cliquant sur « Save », puis avons sélectionné « Apply changes » pour appliquer les changements.



Nous avons ensuite assigné une adresse IP à cette interface afin que les deux pares-feux puissent communiquer via celle-ci.
Pour ce faire, nous avons sélectionné « Static IPv4 » dans la ligne « IPv4 Configuration Type ».

Puis, nous sommes descendus dans la section « Static IPv4 Configuration », où nous avons renseigné l'adresse IP de l'interface dans le champ « IPv4 Address ». Nous avons assigné l'adresse 192.168.1.1 au pare-feu Master et 192.168.1.2 au pare-feu Backup, avant de cliquer sur « Save » pour enregistrer les modifications.

Nous avons répété cette manipulation sur le pare-feu Backup, en assignant l'adresse IP 192.168.1.2 à l'interface de synchronisation.

Test de communication des interfaces Sync :

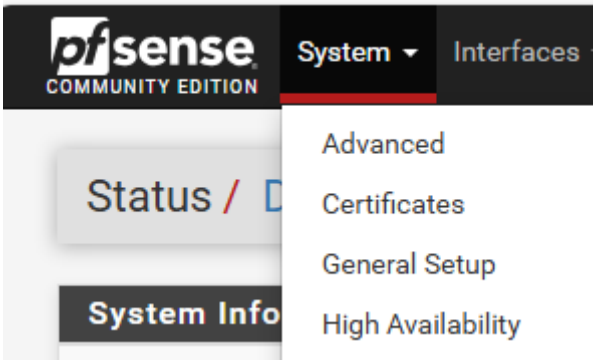
Pour tester la communication, nous sommes retournés dans « Diagnostics », puis « Ping », où nous avons effectué un test de ping depuis l'interface Sync du pare-feu Master vers l'interface Sync du pare-feu Backup, afin de vérifier que les deux pares-feux communiquent correctement via cette interface.
Le test de ping a été concluant et fonctionnel.

```
PING 192.168.1.1 (192.168.1.1) from 192.168.1.2: 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=0.533 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.672 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.491 ms

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.533/0.899/1.491/0.423 ms
```

```
PING 192.168.1.2 (192.168.1.2) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.601 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.681 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.778 ms

--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.601/0.687/0.778/0.073 ms
```

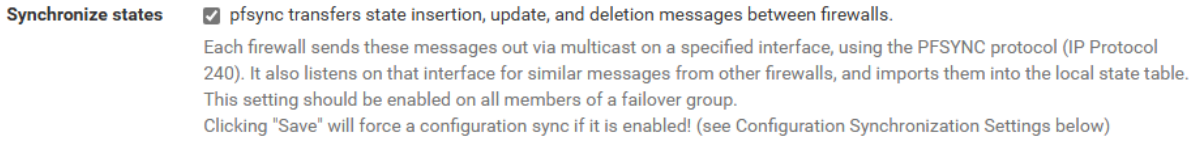
Configuration du HA :

Pour mettre en place le HA sur le pare-feu, nous nous sommes connectés à l'interface web d'administration du pare-feu Master, puis nous sommes allés dans « System », puis « High Availability ».

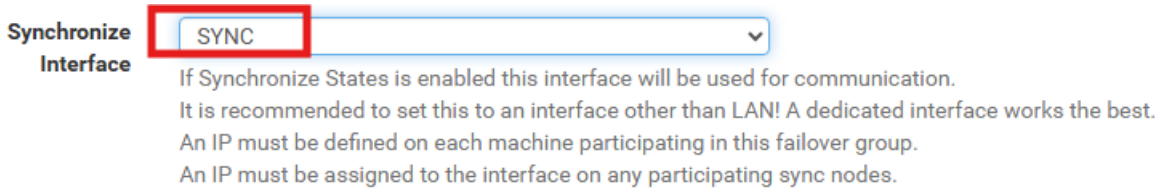


Cela nous a dirigés vers la page de configuration du HA, où j'ai coché la case « Synchronize states ».

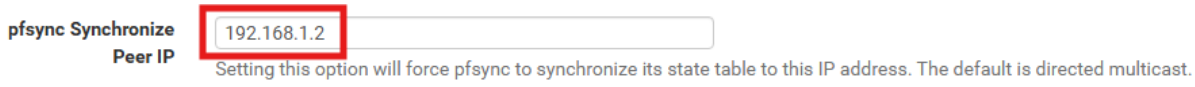
La case « Synchronize States » dans PfSense permet de synchroniser les états de connexion entre les deux pares-feux dans une configuration de haute disponibilité (HA). Cette option garantit une transition fluide lors du basculement entre les nœuds, en maintenant les connexions actives intactes et fonctionnelles, ce qui permet au nœud secondaire de prendre le relais sans perturber les connexions réseau en cours.



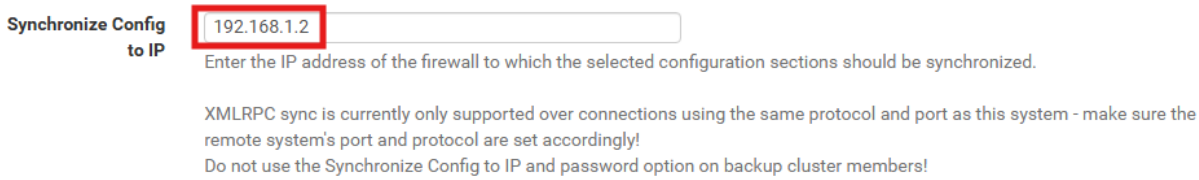
Ensuite, sur la ligne « Synchronize interface », nous avons sélectionné l'interface « Sync ».
Cette ligne permet de spécifier l'interface sur laquelle le HA va se synchroniser.



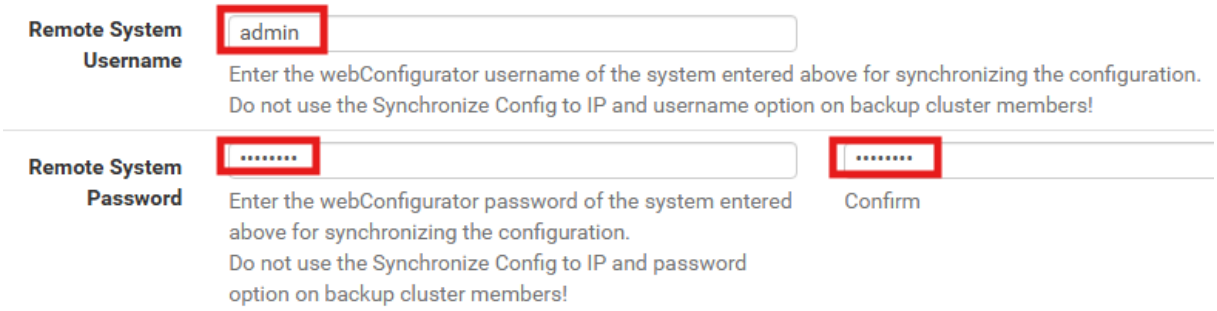
Ensuite, sur la ligne « pfsync synchronize peer IP », nous avons renseigné l'adresse IP de l'interface Sync du pare-feu Backup.
Cette ligne permet au pare-feu Master de synchroniser sa table d'état directement avec l'adresse IP que nous avons spécifiée.



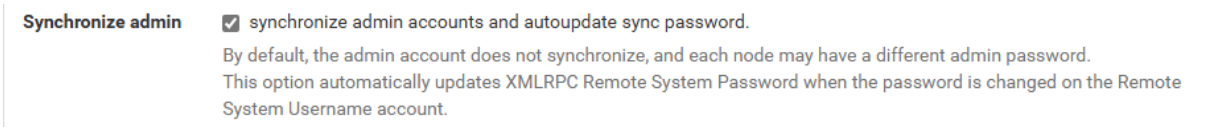
À la ligne suivante, dans « Synchronize Config to IP », nous avons inséré l'adresse IP du pare-feu Backup.
Cette ligne permet de spécifier l'adresse IP du pare-feu sur laquelle seront synchronisées toutes les configurations sélectionnées dans les étapes suivantes.



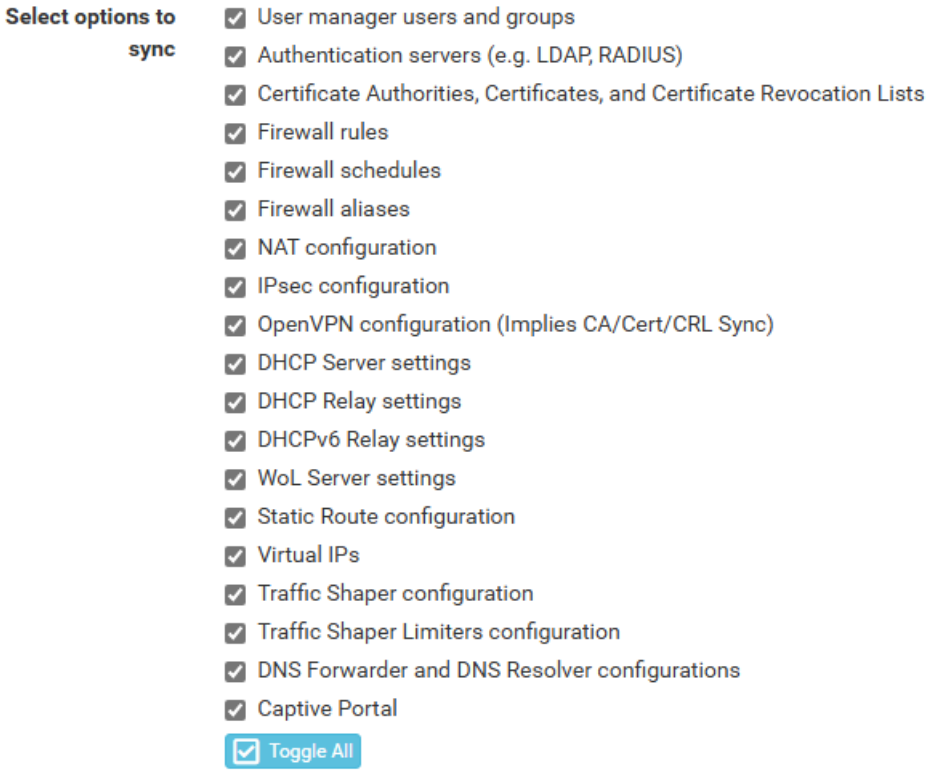
Puis, dans « Remote System Username » et « Remote System Password », nous avons renseigné l'identifiant et le mot de passe pour nous connecter au pare-feu Backup, ce qui permettra au pare-feu Master de tout synchroniser sur l'interface web du pare-feu Backup directement en se connectant.



Ensuite, sur la ligne « Synchronize admin », nous avons coché « Synchronize admin accounts and autoupdate sync password ».



Cette ligne permet de synchroniser le compte administrateur (identifiant et mot de passe) sur l'autre pare-feu, ce qui assure qu'en cas de changement de mot de passe ou d'identifiant sur l'un des pares-feux, l'autre pare-feu possède les mêmes informations d'authentification.
Enfin, sur la ligne « Select options to Sync », nous avons coché « Toggle All », ce qui permet de tout sélectionner.



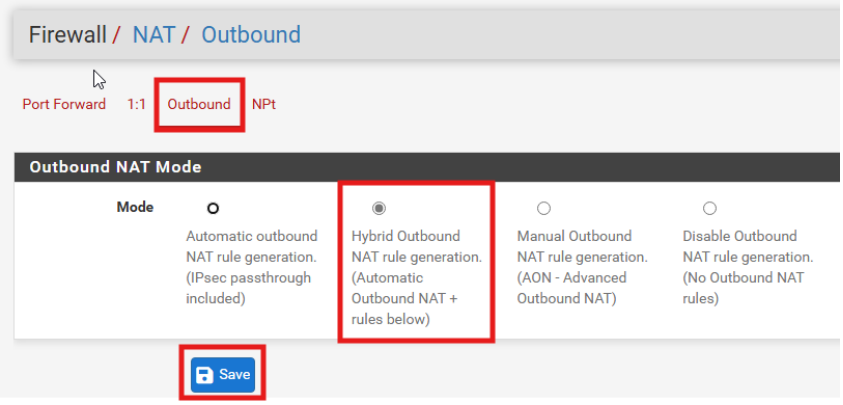
Tout cocher nous permet d'obtenir une réplication complète de notre pare-feu sur le Backup.
Ensuite, nous avons cliqué sur « Save » pour enregistrer les modifications.

Paramétrage des règles de pare-feu :

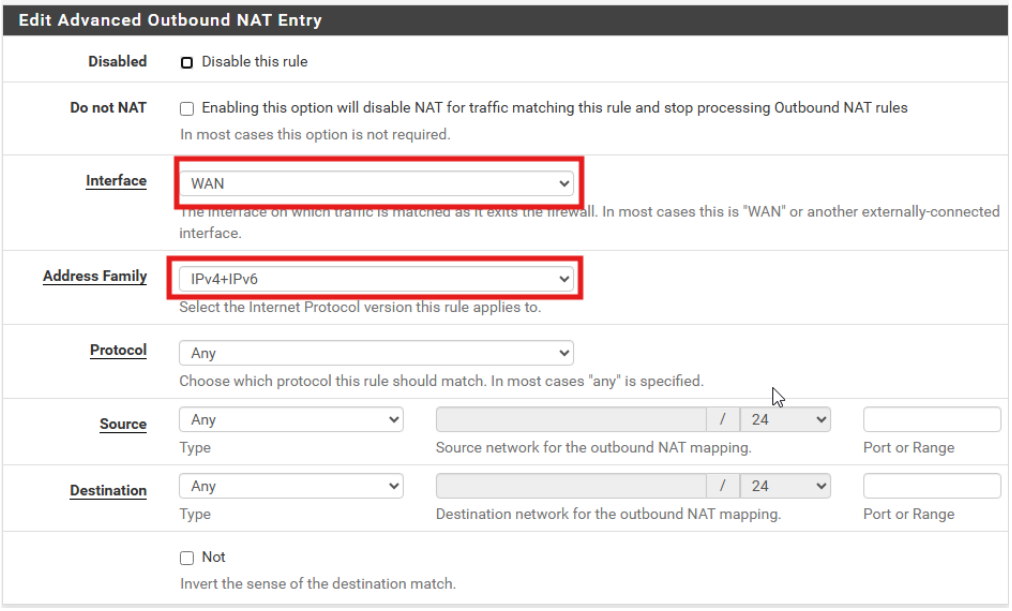
Pour le paramétrage des règles de pare-feu j'ai commencé par créer les une règle de Network Address Translation (NAT) pour que tout ce qui sors de mon par feu soit adresse à l'adresse de mon Wan.

Réglage du NAT :

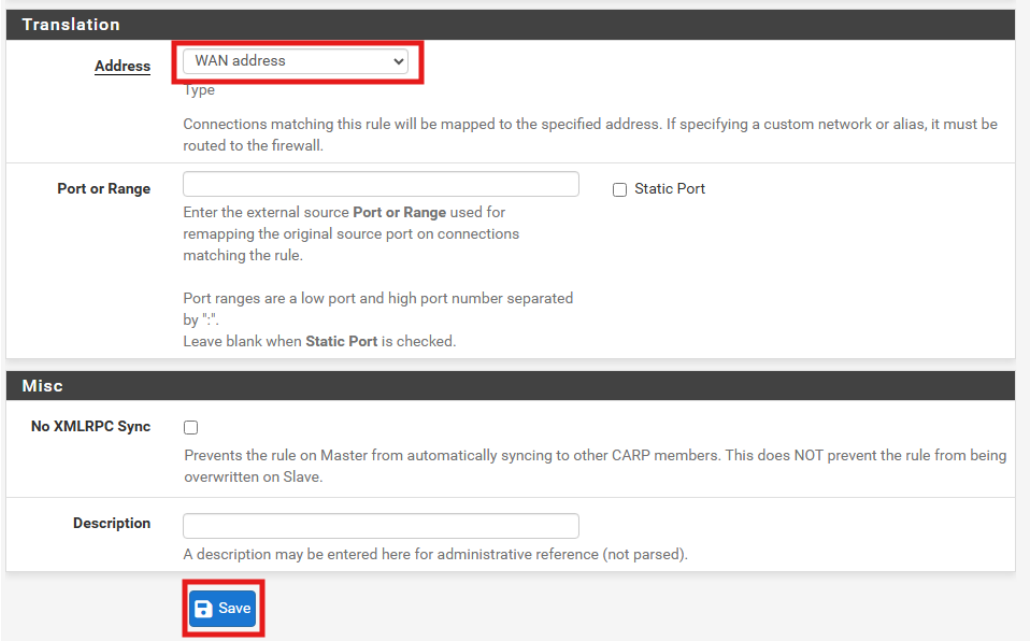
Nous avons cliqué sur le menu « Firewall » puis « NAT ».
Ensuite, nous avons sélectionné l'onglet « Outbound » et activé le mode « Hybrid ». Le mode hybride permet de combiner des règles de NAT manuelles et automatiques, offrant ainsi plus de flexibilité pour gérer les connexions sortantes. Ce mode est particulièrement utile lorsque nous souhaitons personnaliser certaines règles NAT tout en permettant à PfSense de gérer automatiquement les autres connexions sortantes.
Après avoir activé ce mode, nous avons cliqué sur les boutons « Save » et « Apply Changes » pour valider les modifications.



Nous avons cliqué à nouveau sur le menu « Firewall » puis « NAT ».
Nous avons sélectionné l'onglet « Outbound ».
Dans la rubrique « Mappings », nous avons cliqué sur le bouton vert « Add », puis nous avons sélectionné l'interface WAN dans la ligne « Interface » et choisi « IPV4+IPV6 » dans « Address Family ».



Nous avons ensuite, dans l'onglet « Translation », sélectionné « WAN address » dans le champ « Address ».
Nous avons choisi l'adresse WAN car cela permet de masquer l'adresse IP interne du pare-feu et de faire en sorte que tout le trafic sortant utilise l'adresse IP publique du WAN. Cela permet également d'assurer que toutes les connexions sortantes depuis le réseau interne passent par l'interface WAN, garantissant ainsi que le trafic bénéficie du routage correct et que l'adresse source soit correctement traduite en adresse publique.



Attention à ne pas cocher No XMLRPC Sync sinon la Synchronisation ne fonctionnera pas.

Ensuite, nous avons cliqué sur « Save » pour enregistrer les modifications.

Nous allons maintenant configurer les règles nécessaires au bon fonctionnement de la haute disponibilité en paramétrant les différents flux autorisés dans le pare-feu :

Création des règles de pare-feu :

REGLE 1 – CONFIGURATION DU PROTOCOLE "pfsync" :

Le protocole pfsync permet de synchroniser en temps réel les états de connexion entre deux pares-feux PfSense en haute disponibilité (HA). Cela garantit la continuité des connexions réseau en cas de basculement. Pour que cette synchronisation fonctionne, il est nécessaire de créer une règle sur l'interface de synchronisation (Sync) pour autoriser le trafic pfsync.

Nous avons cliqué à nouveau sur le menu « Firewall » puis « Rules ».
Nous avons sélectionné l'interface « Sync » et cliqué sur le bouton vert « Add ».
Dans la section « Edit Firewall Rule », nous avons choisi « Pass » dans le champ « Action » afin d'autoriser le trafic.

Ensuite, nous avons sélectionné l'interface « Sync » pour indiquer à PfSense que la règle doit s'appliquer sur cette interface.
Nous avons choisi « IPv4 » dans le champ « Address Family » et « PFSYNC » dans le champ « Protocol » pour autoriser spécifiquement le trafic de synchronisation.

Dans le champ « Source », nous avons sélectionné « SYNC subnet » afin d'indiquer que la règle s'applique au réseau sync.
Dans le champ « Destination », nous avons choisi « This Firewall (self) » pour préciser que le trafic est destiné au pare-feu lui-même.

Nous avons cliqué sur les boutons « Save » puis « Apply Changes » afin de valider la règle autorisant le protocole CARP.

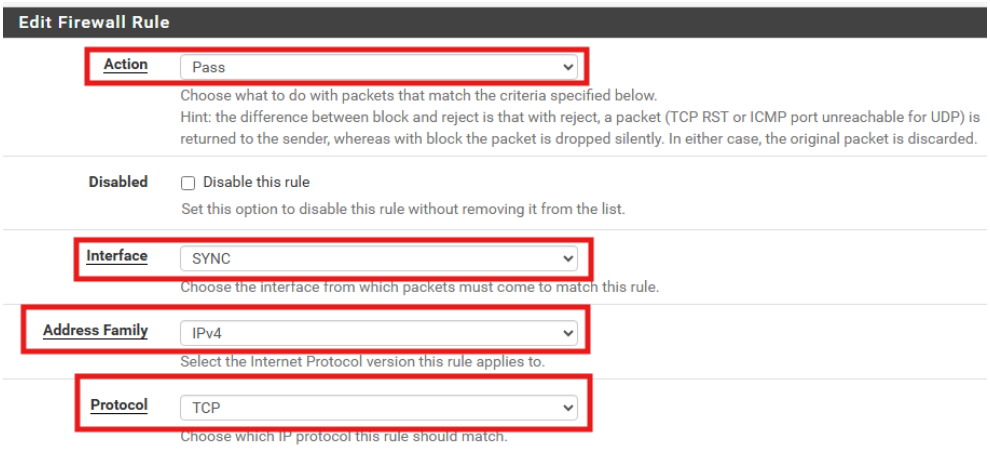
En résumé, cette règle permet de faire circuler, sur l'interface Sync, le protocole PFSYNC depuis le réseau de synchronisation (Sync subnet) vers le pare-feu lui-même.

REGLE 2 – CONFIGURATION DU PROTOCOLE "XML-RPC" :

Le protocole XML-RPC permet de synchroniser automatiquement la configuration du pare-feu principal vers le pare-feu secondaire dans une architecture HA sous PfSense. Pour que cette synchronisation fonctionne, il est nécessaire de créer une règle sur l'interface de synchronisation (Sync) pour autoriser le trafic HTTPS (port 443) utilisé par XML-RPC.

Nous avons cliqué sur le bouton vert « Add » pour ajouter la deuxième règle.
Dans la section « Edit Firewall Rule », nous avons sélectionné les mêmes paramètres

que pour la règle précédente, à l'exception du protocole, où nous avons choisi TCP, un protocole de transport.



Dans le champ « Source »et « Destination », nous avons sélectionné les mêmes paramètres que pour la règle précédente, à l'exception que nous avons sélectionner le port 443 (HTTPS) dans « Destination Port Range ».

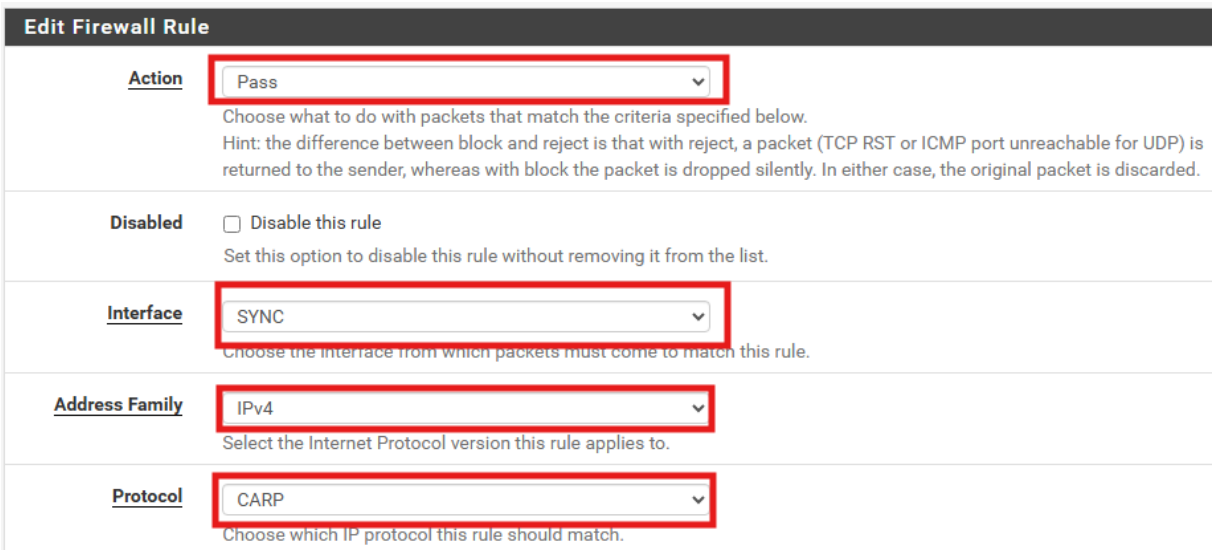
Nous avons cliqué sur les boutons « Save » puis « Apply Changes » pour valider la règle autorisant le flux XML-RPC.

En résumé, cette règle permet de faire circuler, sur l'interface Sync, le protocole TCP sur le port 443 (HTTPS) depuis le réseau de synchronisation (Sync subnet) vers le pare-feu lui-même.

REGLE 3 – CONFIGURATION DU PROTOCOLE "CARP" :

Le protocole CARP permet à plusieurs pares-feux de partager une adresse IP virtuelle pour assurer la haute disponibilité (HA). En cas de panne du pare-feu principal, le pare-feu secondaire prend le relais, garantissant ainsi la continuité des services. Une règle de pare-feu est nécessaire pour permettre le trafic CARP entre les pares-feux et assurer le bon fonctionnement de cette transition automatique.

Nous avons cliqué sur le bouton vert « Add » pour ajouter la troisième règle. Dans la section « Edit Firewall Rule », nous avons sélectionné les mêmes paramètres que pour la règle précédente, à l'exception du protocole, où nous avons choisi CARP.



Dans le champ « Source », nous avons sélectionné les mêmes paramètres que pour la règle précédente. Dans le champ « Destination », nous avons sélectionné « Any », ce qui permet à la règle de s'appliquer à toutes les destinations, assurant ainsi que le trafic CARP puisse circuler sans restriction entre les pares-feux.

Nous avons cliqué sur les boutons « Save » puis « Apply Changes » pour valider la règle autorisant le flux CARP sur l'interface SYNC.

En résumé, cette règle permet de faire circuler, sur l'interface Sync, le protocole CARP depuis le réseau de synchronisation (Sync subnet) vers toutes les destinations, garantissant ainsi la communication entre les pares-feux pour assurer la haute disponibilité.

REGLE 4 – CONFIGURATION DE LA PASSERELLE UNIQUE SUR LE RESEAU "LAN" :

Cette règle permet à l'interface LAN d'utiliser en permanence la passerelle unique fournie par la Fab Academy pour accéder à Internet. Cela garantit une connectivité constante et centralisée, simplifiant ainsi la gestion réseau et assurant une configuration cohérente sur l'ensemble des systèmes hébergés.

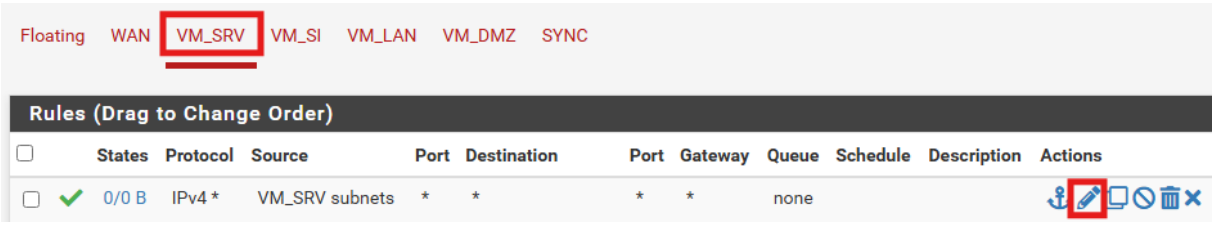
Dans le menu "System" > "Routing", nous avons sélectionné l'onglet "Gateways" puis cliqué sur le bouton vert "Add" pour ajouter une nouvelle passerelle sur le pare-feu.

Dans le champ « Interface », nous avons sélectionné l'interface WAN, et dans « Address Family », nous avons choisi IPv4.
Ensuite, dans le champ « Name », nous avons saisi « Gateway » pour nommer la passerelle, et dans le champ « Gateway », nous avons renseigné l'adresse IP du routeur le plus proche : 10.0.85.254.

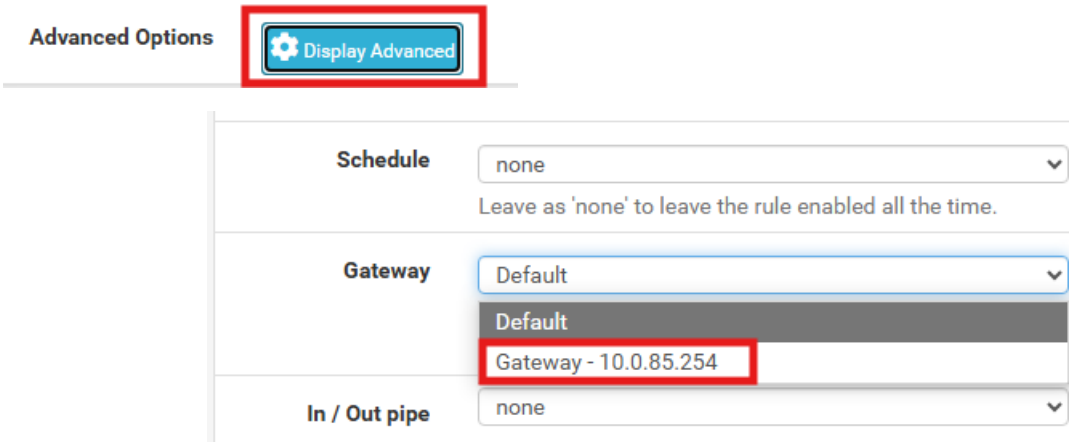
Nous avons cliqué sur les boutons « Save » puis « Apply Changes » afin de valider l'ajout de la nouvelle passerelle par défaut.

Maintenant, nous allons modifier la règle de trafic sortant du "LAN" de manière à intégrer cette passerelle unique.

Dans "Firewall" – "Rules" sur l'interface "VM_SRV" nous avons éditez la règle qui permet de faire circuler tout le trafic réseau depuis VM_SRV vers tout le monde.



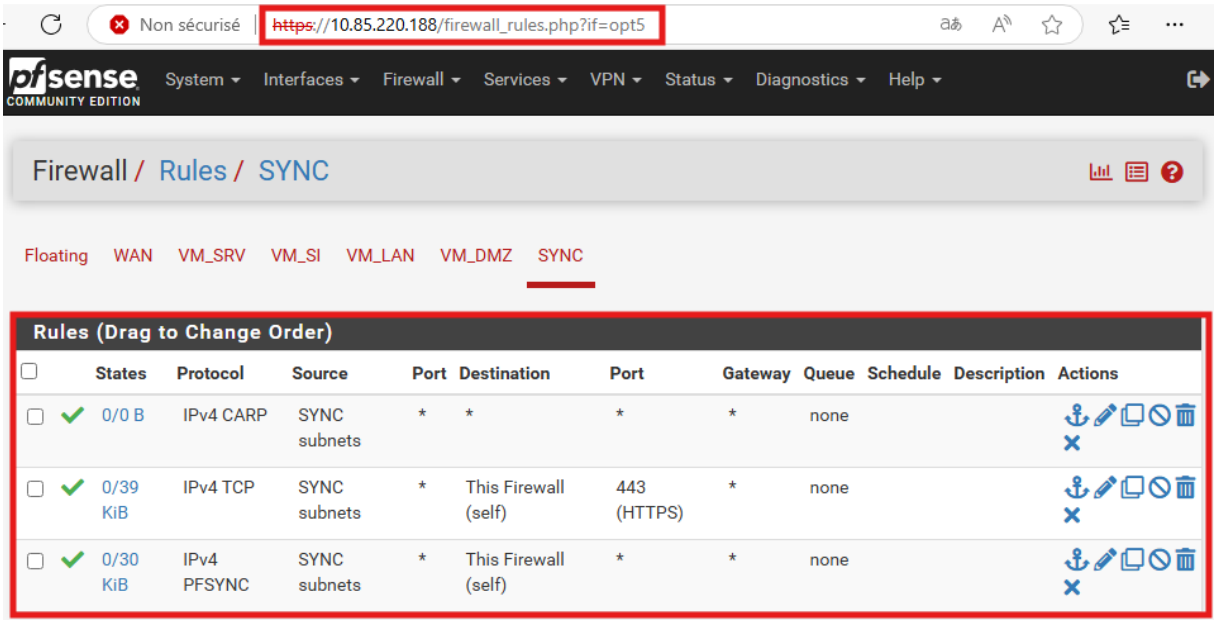
Pour intégrer cette nouvelle passerelle, nous avons cliqué sur « Display Advanced » dans la section « Advanced Options », ce qui a permis d'afficher des options supplémentaires. Parmi elles, nous avons trouvé l'option « Gateway », dans laquelle nous avons sélectionné la nouvelle passerelle précédemment créée, nommée « Gateway ». Cela permet d'associer explicitement cette passerelle à la règle.



Nous avons cliqué sur les boutons « Save » puis « Apply Changes » afin de valider la modification de la règle.
Nous avons ensuite constaté que le nom de la nouvelle passerelle apparaît désormais sur la règle, confirmant ainsi qu'elle est bien prise en compte pour le routage du trafic associé.

Test de fonctionnement du HA :

Pour vérifier le bon fonctionnement du HA, nous sommes allés sur le pare-feu Backup, dans le menu « Firewall » > « Rules », puis sur l'interface « Sync », afin de vérifier que les règles avaient bien été copiées depuis le pare-feu Master.



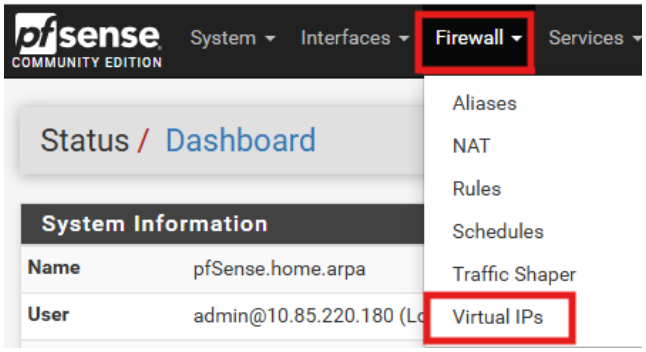
Nous avons pu constater que toutes les règles avaient bien été créées sur le pare-feu Backup.
Maintenant que l'ensemble des règles est en place sur les deux pare-feux et que le HA est fonctionnel, nous allons passer à la création des adresses IP virtuelles (CARP).

Mise en place de l'adresse IP virtuelle WAN :

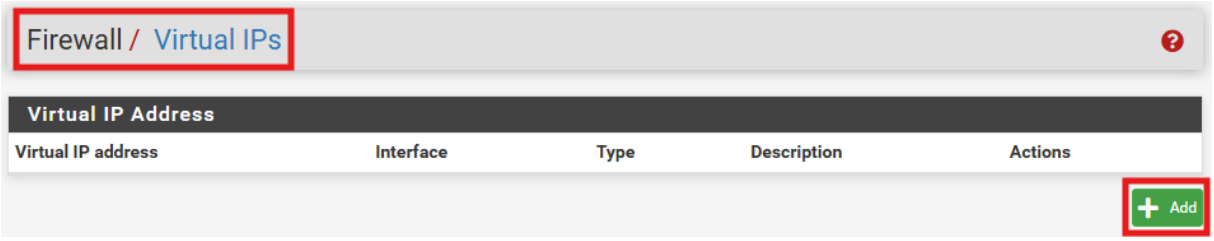
Puisque le HA est désormais en place sur les pares-feux, avec une synchronisation active du pare-feu Master vers le Backup, les étapes suivantes doivent être effectuées uniquement sur le pare-feu Master.
En effet, toutes les configurations que nous allons réaliser seront automatiquement répliquées sur le pare-feu secondaire grâce au mécanisme de synchronisation.

Nous avons commencé par créer l'adresse IP virtuelle WAN, qui servira de passerelle unique pour le trafic sortant.

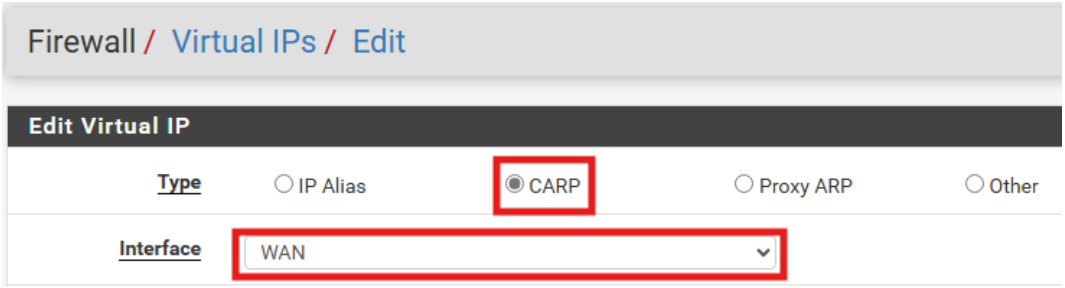
Pour cela, nous nous sommes rendus dans le menu « Firewall », puis « Virtual IPs », afin de configurer une adresse IP partagée (CARP) entre les deux pares-feux.



Ensuite, nous avons cliqué sur « ADD » pour l'ajouter.

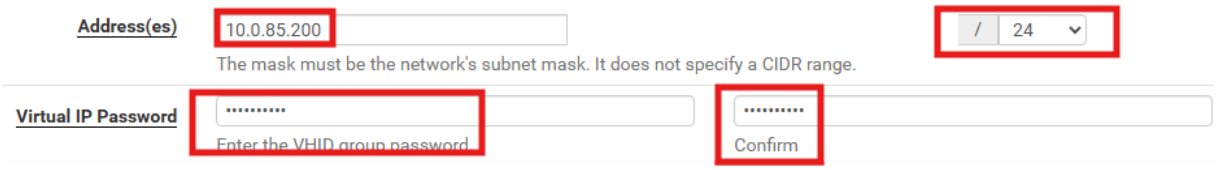


Nous avons sélectionné « CARP » sur la première ligne pour définir le type d'adresse IP virtuelle.
Ensuite, sur la ligne « Interface », nous avons choisi l'interface WAN, car l'adresse IP virtuelle sera associée à cette interface pour gérer le trafic sortant.



Puis, dans la ligne « Address », nous avons saisi l'IP virtuelle pour l'interface CARP WAN, c'est-à-dire 10.0.85.200/24, car cette adresse doit être dans le même sous-réseau que la passerelle, qui est en 10.0.85.254/24.

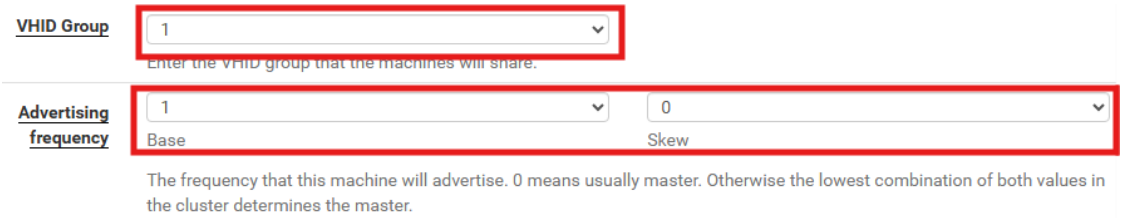
Ensuite, dans la ligne « Virtual IP Password », nous avons entré un mot de passe, spécifiquement destiné à la gestion des adresses IP virtuelles, afin de sécuriser la communication entre les nœuds du HA pour cette adresse IP.



Sur la ligne VHID group, nous avons laissé la valeur 1, car il s'agit de la première adresse IP virtuelle que nous avons créée. Pour les adresses suivantes, il faudra définir un numéro de groupe VHID unique, comme 2 pour la deuxième adresse IP virtuelle.

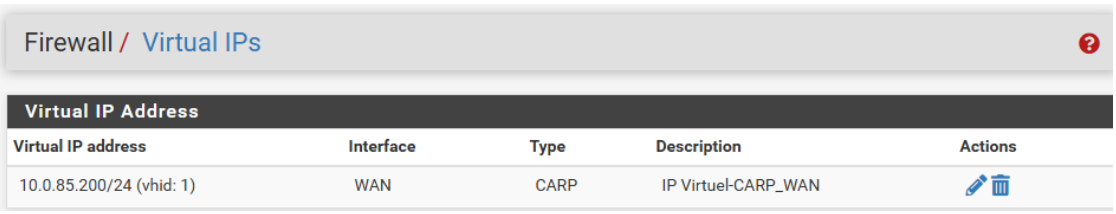
Dans la section « Advertising frequency », nous avons laissé « Base » à 1 et « Skew » à 0, ce qui indique au pare-feu principal qu'il est le maître de la redondance. Le Skew à 0 permet au pare-feu primaire d'avoir une priorité plus élevée lors de la gestion de l'adresse IP virtuelle.

Lors de la synchronisation sur le pare-feu secondaire (Backup), ces paramètres seront copiés, à l'exception du Skew, qui sera automatiquement ajusté à 100. Cela signalera au pare-feu secondaire qu'il est configuré comme le pare-feu de secours et qu'il doit prendre le relais uniquement si le pare-feu principal devient indisponible.



Enfin, nous avons ajouté une description pour indiquer qu'il s'agissait de l'adresse IP virtuelle WAN, en utilisant le nom IP Virtuelle-CARP_WAN. Nous avons ensuite enregistré et appliqué les modifications.

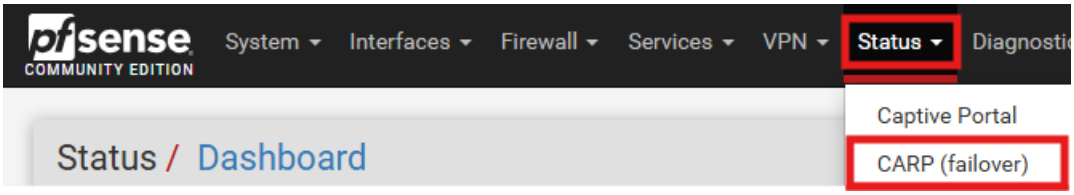
Nous pouvons désormais retrouver l'adresse IP virtuelle que nous avons créée dans le menu Firewall > Virtual IPs, où elle sera listée et pourra être consultée ou modifiée si nécessaire.



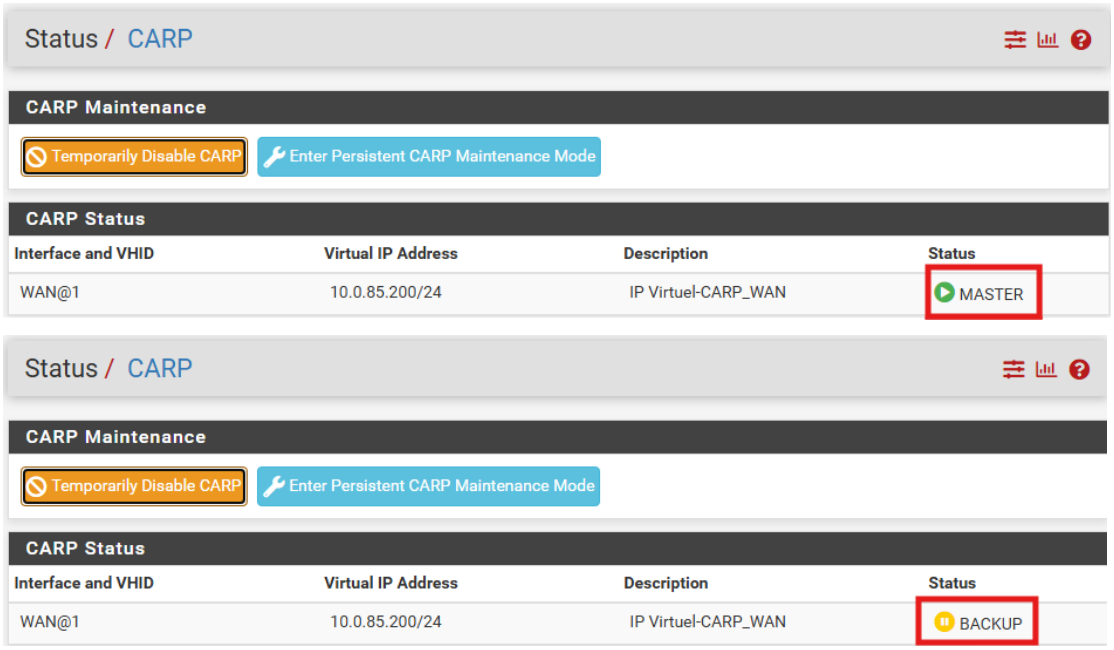
Vérification MASTER / BACKUP :

Après la configuration de l'adresse IP virtuelle, nous avons vérifié que le pare-feu Master était bien en mode principal (master), et que le pare-feu Backup avait correctement synchronisé cette adresse IP virtuelle tout en se mettant en mode de secours (backup).

Pour ce faire, nous sommes allés dans « Status », puis dans « CARP Failover ». Cette page nous a permis de vérifier l'état du basculement CARP, afin de confirmer que la configuration HA fonctionnait comme prévu et que les deux pares-feux étaient bien synchronisés.

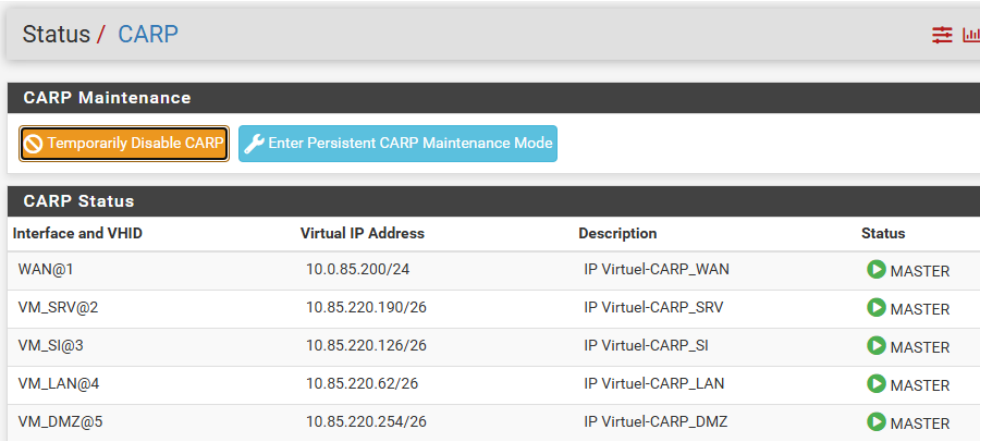


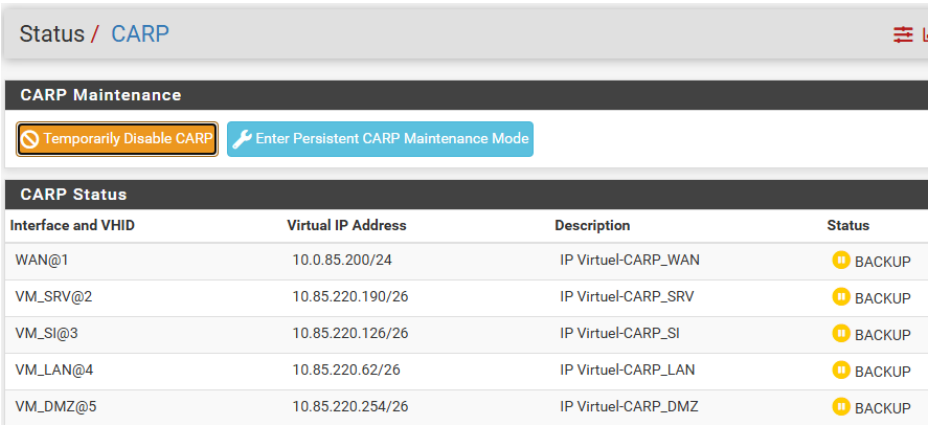
Nous avons alors constaté que sur le pare-feu Master, l'adresse IP CARP était bien indiquée avec le statut « Master », tandis que sur le pare-feu Backup, l'adresse IP CARP affichait le statut « Backup ». Cela confirme que la configuration HA est correcte et que la synchronisation entre les deux pares-feux fonctionne comme prévu.



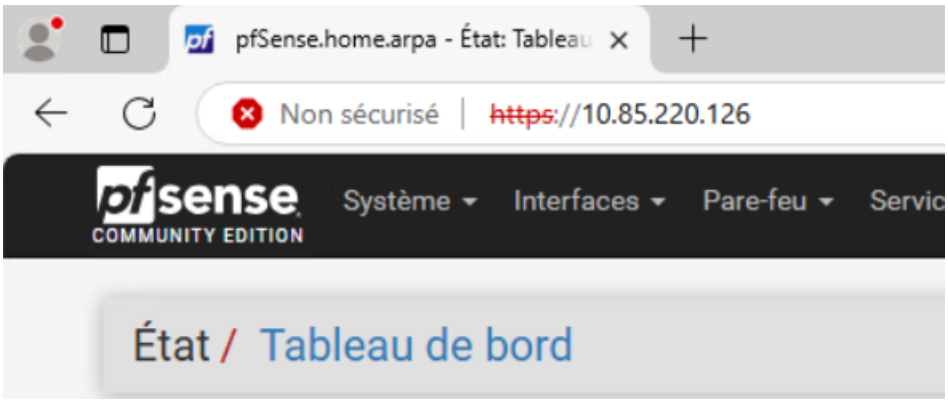
Configuration Final :

Après cette vérification, nous avons configuré les quatre autres adresses IP virtuelles de la même manière que précédemment.





Pour finir la mise en place du CARP, nous avons vérifié l'accès au web de l'interface SI. Pour ce faire, nous avons ouvert un navigateur et saisi l'URL suivante : https://10.85.220.126.

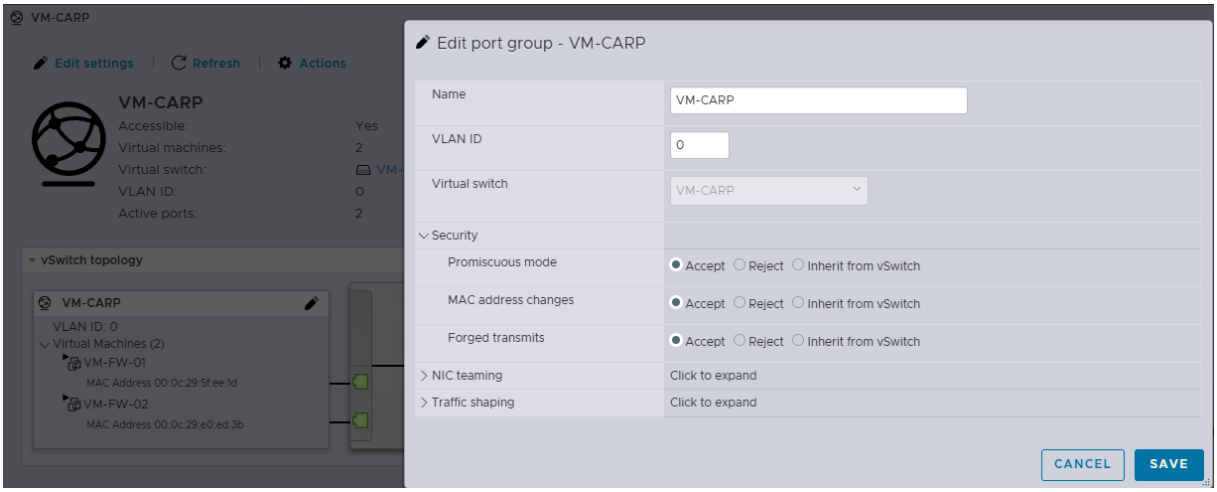


Nous pouvons constater que l'adresse IP CARP du VLAN SI fonctionne, car nous avons pu accéder à son interface de synchronisation.

Difficultés rencontrées :

Master / Backup :

Nous avons rencontré des difficultés lors de la mise en place des adresses IP virtuelles, car les deux pares-feux indiquaient l'état "MASTER" dans l'interface « *Status* > *CARP* ».
Ce problème provenait de l'hyperviseur ESXi : dans les paramètres de sécurité des groupes de ports, les options "Promiscuous mode", "MAC address changes" et "Forged transmits" étaient réglées sur "Reject".
Après avoir modifié ces paramètres en les passant sur "Accept", le pare-feu secondaire est bien passé en mode "BACKUP", ce qui a permis au mécanisme de basculement de fonctionner correctement.



Accès internet :

Nous avons également rencontré des difficultés lors de la configuration de l'adresse IP virtuelle (CARP) WAN. Initialement, nous avions configuré cette adresse en 10.0.24.254, soit la dernière adresse disponible dans le réseau WAN.
Cependant, cette configuration nous empêchait d'accéder à Internet.

Après analyse, nous avons identifié que le problème venait de l'adressage de l'IP virtuelle (CARP) WAN : pour fonctionner correctement, cette adresse doit impérativement se situer dans le même sous-réseau que la passerelle.

Nous avons donc réassigné l'adresse IP virtuelle à 10.0.85.200, en cohérence avec la passerelle, et l'accès à Internet a été rétabli.

Amélioration possible :

Pour l'entreprise Dualya, compte tenu de sa taille et de sa croissance, le groupe HAssistance propose les améliorations suivantes :

Routeur avec redondance :

La mise en place de deux routeurs en redondance, afin d'isoler le service de routage de celui assuré par les pares-feux.

Cette séparation permettrait, en cas de défaillance d'un équipement (routeur ou pare-feu), de ne rétablir que le service concerné, sans impacter les autres fonctions critiques comme le filtrage des paquets.

Server VPN :

Le groupe HAssistance propose également à l'entreprise Dualya la mise en place d'un serveur VPN de type "Client to Site".
Cette solution permettrait aux employés de travailler à distance.

Actuellement, seuls une solution VPN "Site to Site" est configurés sur les pares-feux. Or, avec la croissance de l'entreprise, il est probable que Dualya ait prochainement besoin d'une solution "Client to Site" pour offrir plus de flexibilité à ses collaborateurs.

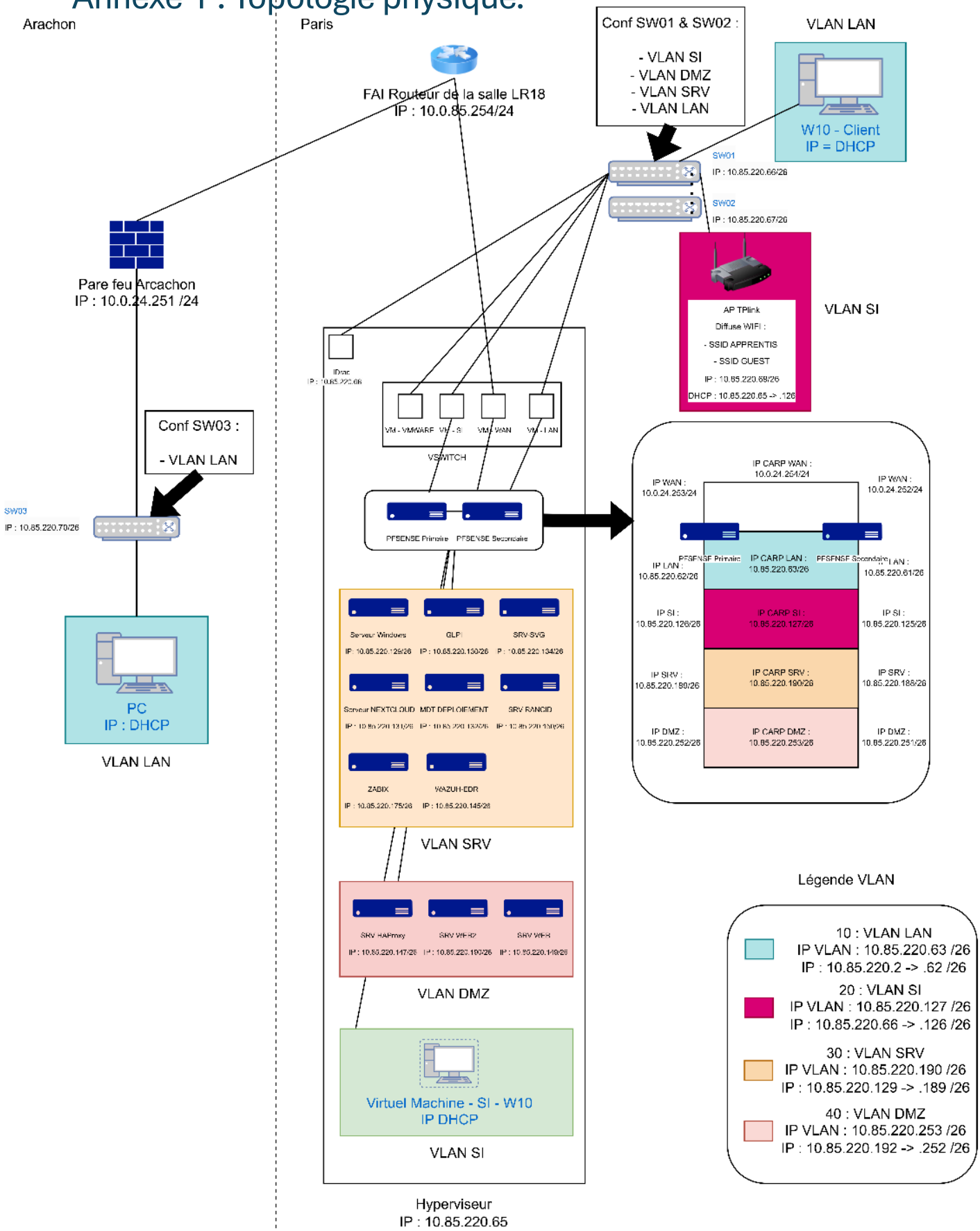
Conclusion :

Pour conclure, ce dossier nous a permis d'explorer les différentes étapes nécessaires à la mise en place de la redondance des pares-feux.
Cette démarche, bien que ponctuée de difficultés, nous a permis de les surmonter avec succès, tout en élargissant notre compréhension des infrastructures réseau.
Grâce à cette expérience, nous sommes désormais en mesure de proposer des améliorations pertinentes et adaptées aux besoins de l'entreprise Dualya.

Vous pouvez retrouver ce dossier dans mon portefolio via l'adresse suivante :

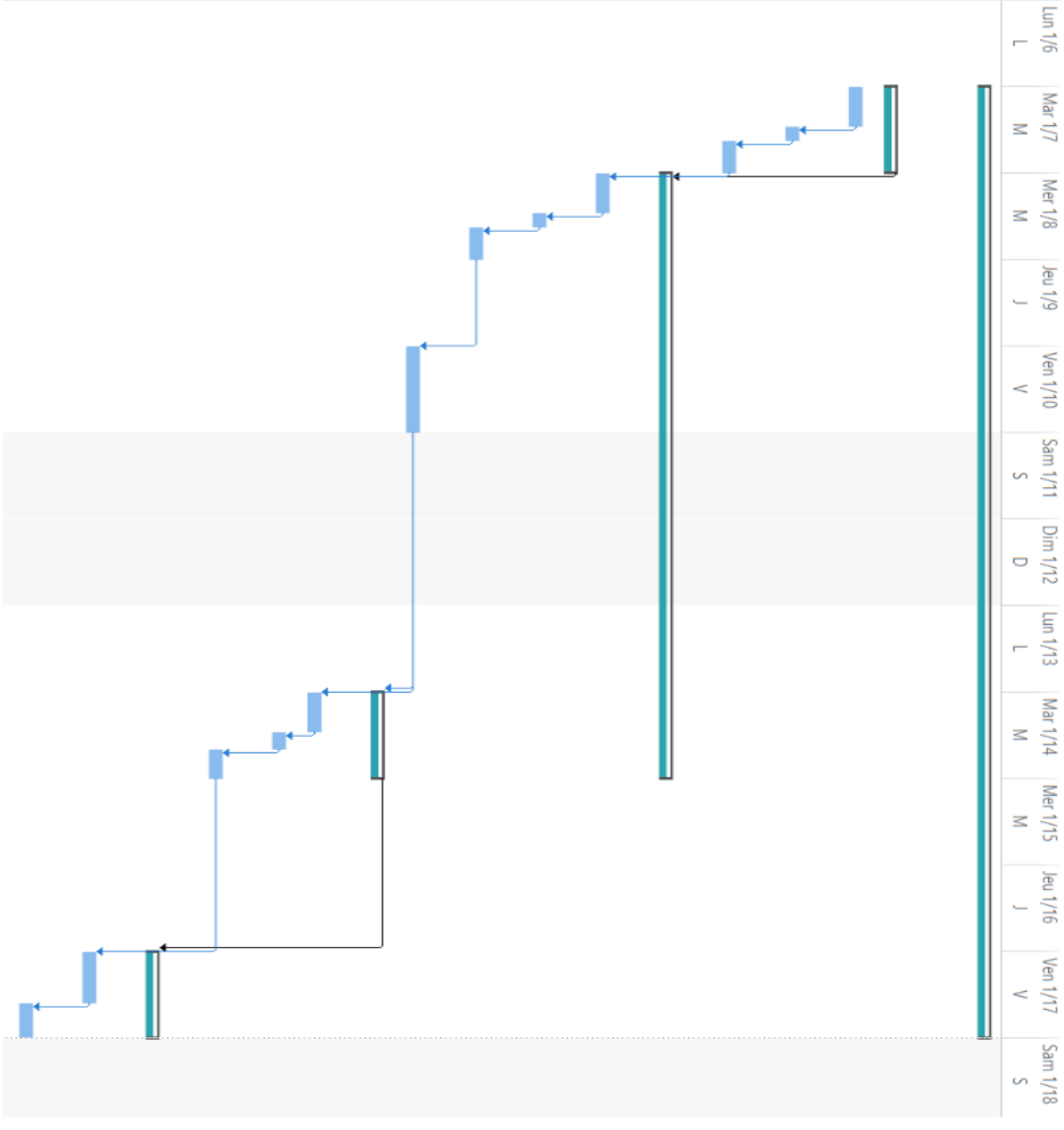
https://nicolas.hachet.formation-esiac.fr

Annexe 1 : Topologie physique.



Annexe 2 : Schéma de Gantt.

Mode Tâche	Nom de la tâche	Durée	Début	Fin
	Mise en place de la haute disponibilité pour les pares-feux PfSense	**9 jours**	**Mar 1/7/25**	**Ven 1/17/25**
	Préparation des pares-feux	**1 jour**	**Mar 1/7/25**	**Mar 1/7/25**
	Vérification de l'heure sur le pare-feu	0.3 jour	Mar 1/7/25	Mar 1/7/25
	Vérification que le système est à jour	0.3 jour	Mar 1/7/25	Mar 1/7/25
	Vérification de l'accès internet	0.4 jour	Mar 1/7/25	Mar 1/7/25
	Mise en place du HA sur le pare-feu Master	**5 jours**	**Mer 1/8/25**	**Mar 1/14/25**
	Création de l'interface de synchronisation	0.3 jour	Mer 1/8/25	Mer 1/8/25
	Configuration de l'interface de synchronisation	0.3 jour	Mer 1/8/25	Mer 1/8/25
	Test de communication des interfaces Sync	0.4 jour	Mer 1/8/25	Mer 1/8/25
	Configuration du HA	1 jour	Ven 1/10/25	Ven 1/10/25
	Paramétrage des règles de pare-feu	**1 jour**	**Mar 1/14/25**	**Mar 1/14/25**
	Réglage du NAT	0.3 jour	Mar 1/14/25	Mar 1/14/25
	Création des règles de pare-feu	0.4 jour	Mar 1/14/25	Mar 1/14/25
	Test de fonctionnement du HA	0.3 jour	Mar 1/14/25	Mar 1/14/25
	Mise en place de l'adresse IP virtuelleWAN	**1 jour**	**Ven 1/17/25**	**Ven 1/17/25**
	Vérification MASTER / BACKUP	0.5 jour	Ven 1/17/25	Ven 1/17/25
	Configuration Final	0.5 jour	Ven 1/17/25	Ven 1/17/25



Annexe 3 : Gestionnaire de mot de passe.

Vous retrouverez ci-dessous le tableau de tous les mots de passe disponible sur l'infrastructure :

Ordinateurs :

Nom de l'appareil	Nom d'utilisateur	Mot de passe
VM-W10-01 (virtuelle)	admin	Du@ly@85-HA-W10
PC1 (PC portable)	admin	Du@ly@85-HA-PC1
PC2 (PC portable)	admin	Du@ly@85-HA-PC2

Serveurs :

Nom de l'appareil	**Nom d'utilisateur**	**Mot de passe**
HYPERVISEUR	root	Du@ly@85-HA-ESXI
IDRAC	root	Du@ly@85-HA-IDRAC
VM-SRV-WINDOWS-SERVER-01	administrateur	Du@ly@85-HA-WS
VM-SRV-GLPI-01	tech	Du@ly@85-HA-GLPI
VM-SRV-DEP-01	administrateur	Du@ly@85-HA-DEP
VM-SRV-SVG-01	administrateur	Du@ly@85-HA-SVG
VM-SRV-RANCID-01	administrateur	Du@ly@85-HA-RANCID
VM-DMZ-WEB-01	tech	Du@ly@85-HA-WEB1
VM-DMZ-WEB-02	tech	Du@ly@85-HA-WEB2
VM-SRV-HAPROXY-01	tech	Du@ly@85-HA-HAPROXY
VM-SRV-ZABBIX-01	tech	Du@ly@85-HA-ZABBIX
VM-SRV-NEXTCLOUD-01	tech	Du@ly@85-HA-NEXTCLOUD
VM-SRV-EDR-01	tech	Du@ly@85-HA-EDR

Toutes les machines virtuelles linux disponible dans la liste ci-dessus dispose un utilisateur root pour faire toutes les manipulations administrateur.

Nom d'utilisateur	**Mot de passe**
root	Du@ly@85-HA-R00T

Réseaux :

Nom de l'appareil	Nom d'utilisateur	Mot de passe
SWITCH 1	admin	Du@ly@85-HA-SW1
SWITCH 2	admin	Du@ly@85-HA-SW2
SWITCH 3	admin	Du@ly@85-HA-SW3
VM-FW-01 (PFSENSE PRINCIPAL)	admin	Du@ly@85-HA-FW01
VM-FW-02 (PFSENSE SECONDAIRE)	admin	Du@ly@85-HA-FW02
FORTINET (Site ARCACHON)	admin	Du@ly@85-HA-FORTINET
BORNE WIFI TP-LINK		Du@ly@85-HA-TPLINK
Partage de fichier (SMB)	hassistance	P@ssw0rd

Utilisateurs du domaine AD :

Nom d'utilisateur	Mot de passe
philippe.pastel	Du@1y@85-pp!
pierre.parry	Du@1y@85-pp
ulysse.alain	Du@1y@85-ua!
baptiste.ludwig	Du@1y@85-bl!
jade.caillaux	Du@1y@85-jc!
sophie.ratier	Du@1y@85-sr!
remy.loiseau	Du@1y@85-rl!
pierre.sabord	Du@1y@85-ps!
sacha.lens	Du@1y@85-sl!
jeanne.reil	Du@1y@85-jr
serge.lay	Du@1y@85-sl!
sybille.gautier	Du@1y@85-sg!
helene.varon	Du@1y@85-hv!
pauline.provost	Du@1y@85-pp!
cecilia.claire	Du@1y@85-cc!
yann.bertrand	Du@1y@85-yb!

Interface des sites web :

Nom du service	Nom d'utilisateur	Mot de passe
GLPI	glpi	Du@ly@85-HA-GLPI
NEXTCLOUD	administrateur	Du@ly@85-SUIVANTNUAGE
WAZUH	admin	Du@ly@85-HA-WAZUH