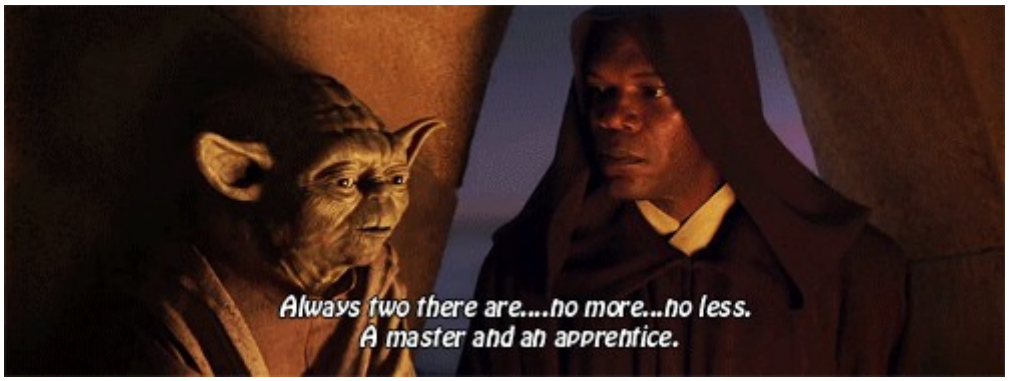
PfSense 2.8.1 // CARP (Common Address Redundancy Protocol)

HAUTE DISPONIBILITÉ (CARP)

Sujet : Implémentation du protocole CARP (Common Address Redundancy Protocol) sur pfSense.

Objectif : Éliminer le SPOF (*Single Point Of Failure*). Assurer la continuité de service en cas de panne matérielle ou logicielle du pare-feu principal.



Cette maxime, bien que tirée d'une galaxie lointaine, illustre parfaitement la philosophie de la **Haute Disponibilité**.

Avoir un seul PfSense, est un **SPOF** (*Single Point Of Failure* - Point Unique de Défaillance).

- **La Situation :** Nous avons un seul "Maître" (pfSense). S'il tombe (panne matérielle, crash update, coupure électrique), c'est le **Blackout**. Fini Netflix (dans le meilleur des cas !).
- **La Solution :** Appliquer la redondance. Nous allons introduire un "Apprenti" (le second nœud pfSense).

L'objectif est de transformer cette faiblesse structurelle en force via le protocole **CARP**. Le noeud secondaire restera dans l'ombre, synchronisant silencieusement les connaissances du Maître (Configuration & États), prêt à prendre le relais instantanément si ce dernier venait à faillir.

L'incident devient alors transparent. L'utilisateur ne voit pas la panne. L’équilibre dans La Force est retrouver.

THÉORIE

Dans une infrastructure classique, si le routeur meurt, le réseau s'effondre. Avec CARP, nous créons un cluster de deux pare-feux (ou plus) qui agissent comme une entité unique.

- **CARP (Le Masque) :** C'est une **Adresse IP Virtuelle (VIP)** partagée. Pour les clients du LAN (Legion, Serveurs), la passerelle est toujours 192.168.110.254. Ils ne savent pas quelle machine physique traite réellement le paquet. Si le Maître tombe, l'Esclave reprend l'IP Virtuelle instantanément.
- **PFSYNC (La Conscience Partagée) :** C'est la synchronisation de la "Table d'États". Si un téléchargement est en cours via le Maître et que celui-ci crashe, l'Esclave connaît déjà l'état de cette connexion (TCP sequence, ports). Résultat : aucune coupure pour l'utilisateur. C'est le "Déjà Vu" de Matrix : un glitch imperceptible.
- **XMLRPC (Le Clonage) :** C'est la synchronisation de la configuration. Une règle créée sur le Maître est automatiquement répliquée sur l'Esclave.

ARCHITECTURE CIBLE & PRÉREQUIS

Avant de toucher à la production, on définit le plan d'adressage. Nous devons modifier les IPs physiques pour libérer l'IP actuelle (.254) afin qu'elle devienne l'IP Virtuelle (VIP).

Rôle	Interface	Machine	IP Physique	IP Virtuelle (VIP / Gateway)
MASTER	WAN (DHCP)	lab-pfsense-01	192.168.100.246	192.168.100.254
BACKUP	WAN (DHCP)	lab-pfsense-02	192.168.100.248	192.168.100.254
MASTER	LAN (STATIC)	lab-pfsense-01	192.168.110.251	192.168.110.254
BACKUP	LAN (STATIC)	lab-pfsense-02	192.168.110.252	192.168.110.254
MASTER	DMZ (STATIC)	lab-pfsense-01	192.168.120.251	192.168.120.254
BACKUP	DMZ (STATIC)	lab-pfsense-02	192.168.120.252	192.168.120.254

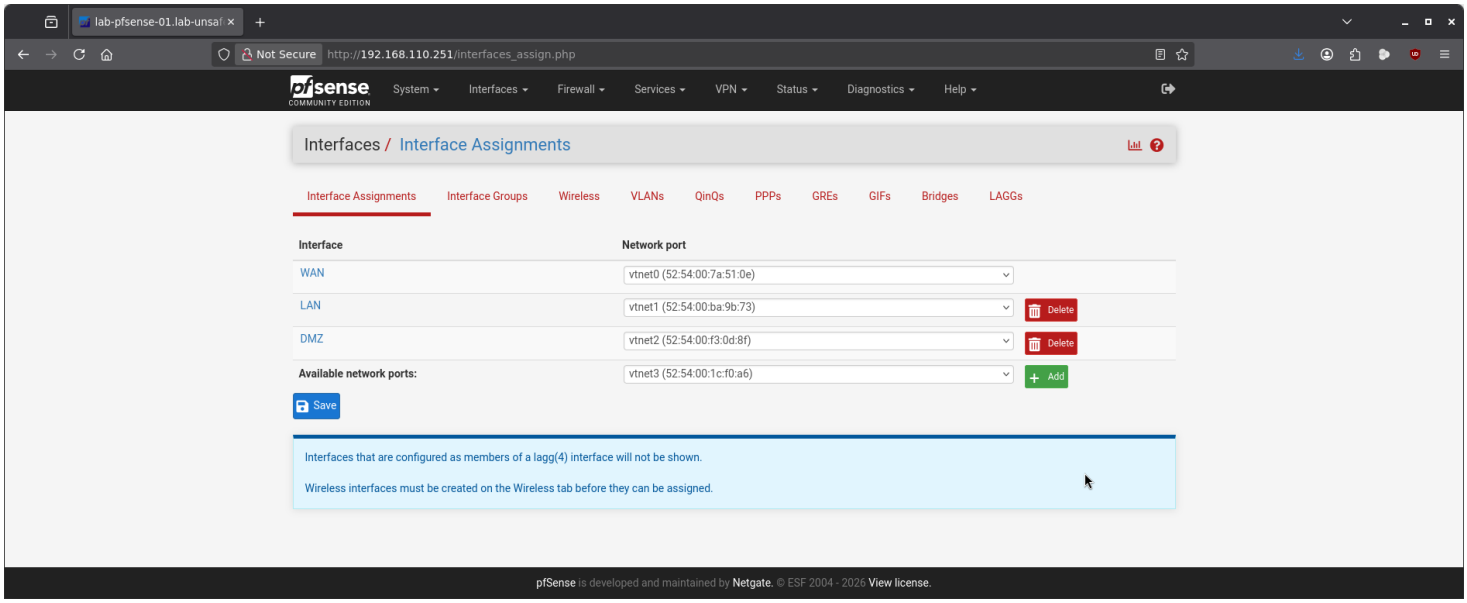
> **ATTENTION :** Si l'infrastructure est virtualisée (VMware, VirtualBox, Proxmox). On **DOIT** activer le **"Promiscuous Mode"** (Mode Promiscuité) et autoriser l'usurpation d'adresse MAC sur les vSwitchs concernés. Sans cela, l'hyperviseur bloquera les paquets CARP (qui utilisent une MAC virtuelle multicast) et le cluster ne fonctionnera jamais.

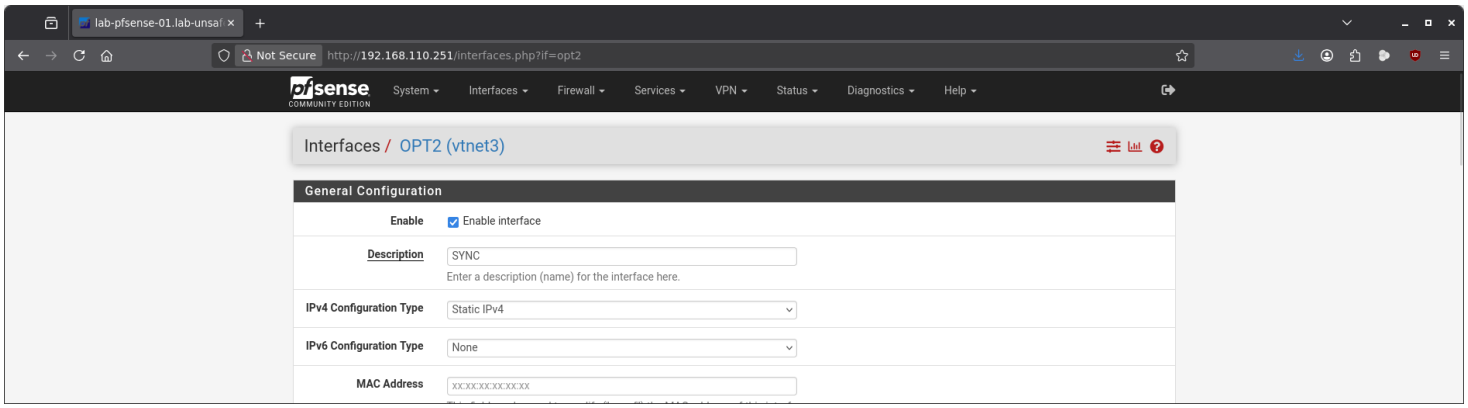
MISE EN PLACE

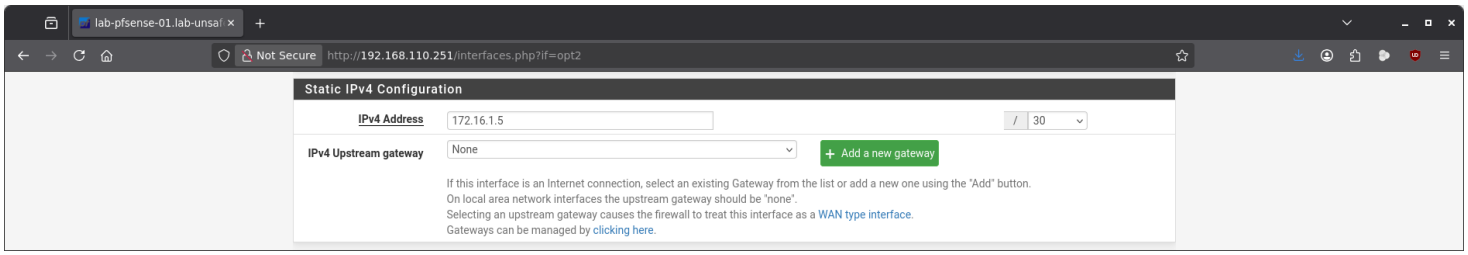
Le Lien de Synchronisation

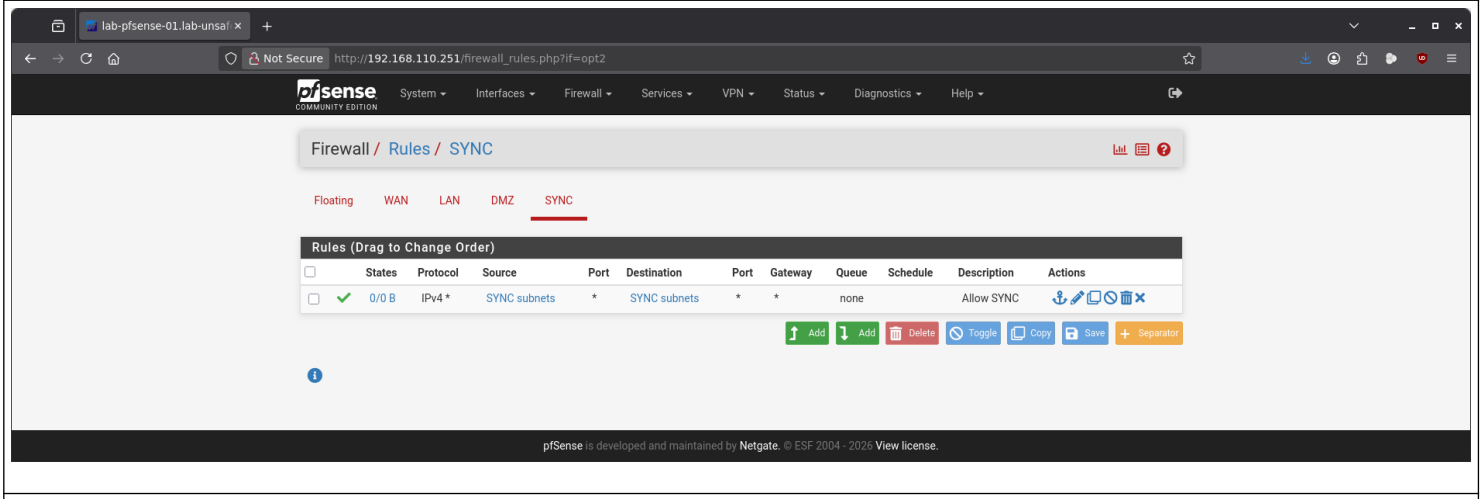
Nous avons besoin d'un lien direct et isolé entre les deux pare-feux pour qu'ils discutent sans polluer le réseau.

- **Sur les deux pfSense :** On ajoute une interface réseau dédiée.
- **Adressage** (Utilisation d'un masque /30 pour restreindre strictement le lien à deux hôtes) :
  - Master : 172.16.1.5 /30
  - Backup : 172.16.1.6 /30
- **Règle Pare-feu (Onglet SYNC) :**
  - On crée une règle autorisant **tout le trafic** (Protocol: ANY, Source: SYNC Net, Dest: SYNC Net).
  - *Note :* Ce lien étant physiquement isolé, cette règle "ouverte" ne présente pas de risque pour le reste du réseau.





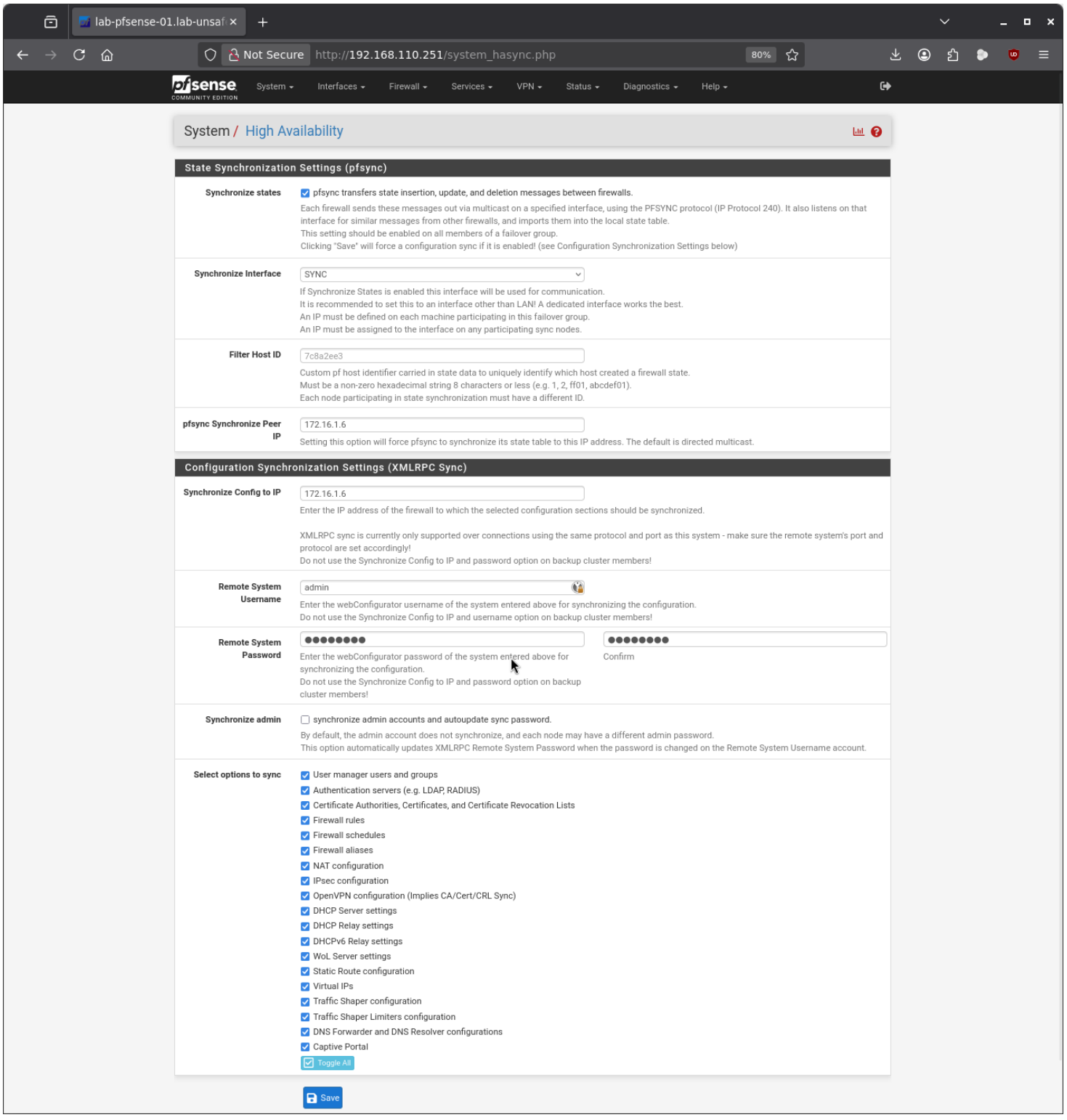




CONFIGURATION DE LA HAUTE DISPONIBILITÉ (HA)

Nous allons maintenant configurer le cerveau du cluster. Cette étape permet au Maître de répliquer sa configuration et ses tables d'états vers l'Esclave.

Sur le MASTER (lab-pfsense-01) Aller dans System > High Avail. Sync

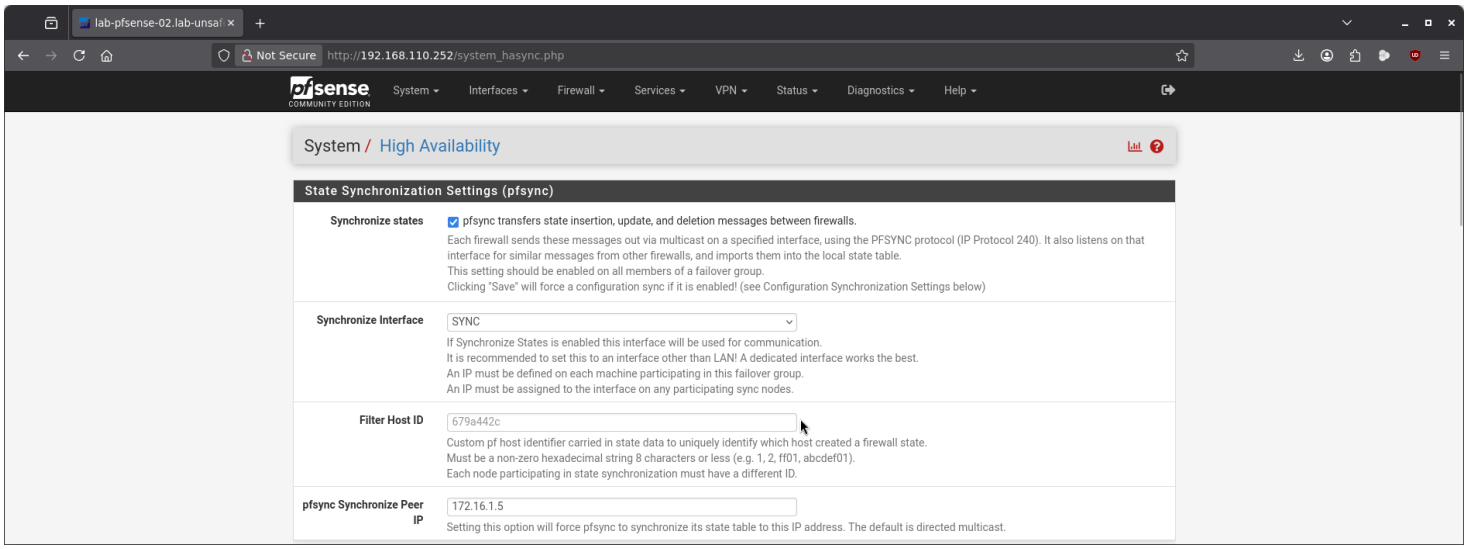


- **Pfsync State Sync (Synchronisation des états) :**
  - Cocher Synchronize States.
  - *Interface* : Sélectionner SYNC.
  - *pfsync Peer IP* : 172.16.1.2 (On pointe vers l'autre bout du tunnel).

- **XMLRPC Sync (Clonage de Configuration) :**
  - *Synchronize Config to IP* : 172.16.1.2
  - *Remote System Username* : admin (L'utilisateur par défaut).
  - *Remote System Password* : (Saisir le mot de passe du pare-feu **BACKUP**).
  - *Select options to sync* : Cocher **Toggle All** (ou sélectionner spécifiquement Rules, VIP, NAT, DHCP, Aliases).

- **Sauvegarder.**

Sur le BACKUP (lab-pfsense-02) Aller dans **System > High Avail. Sync**



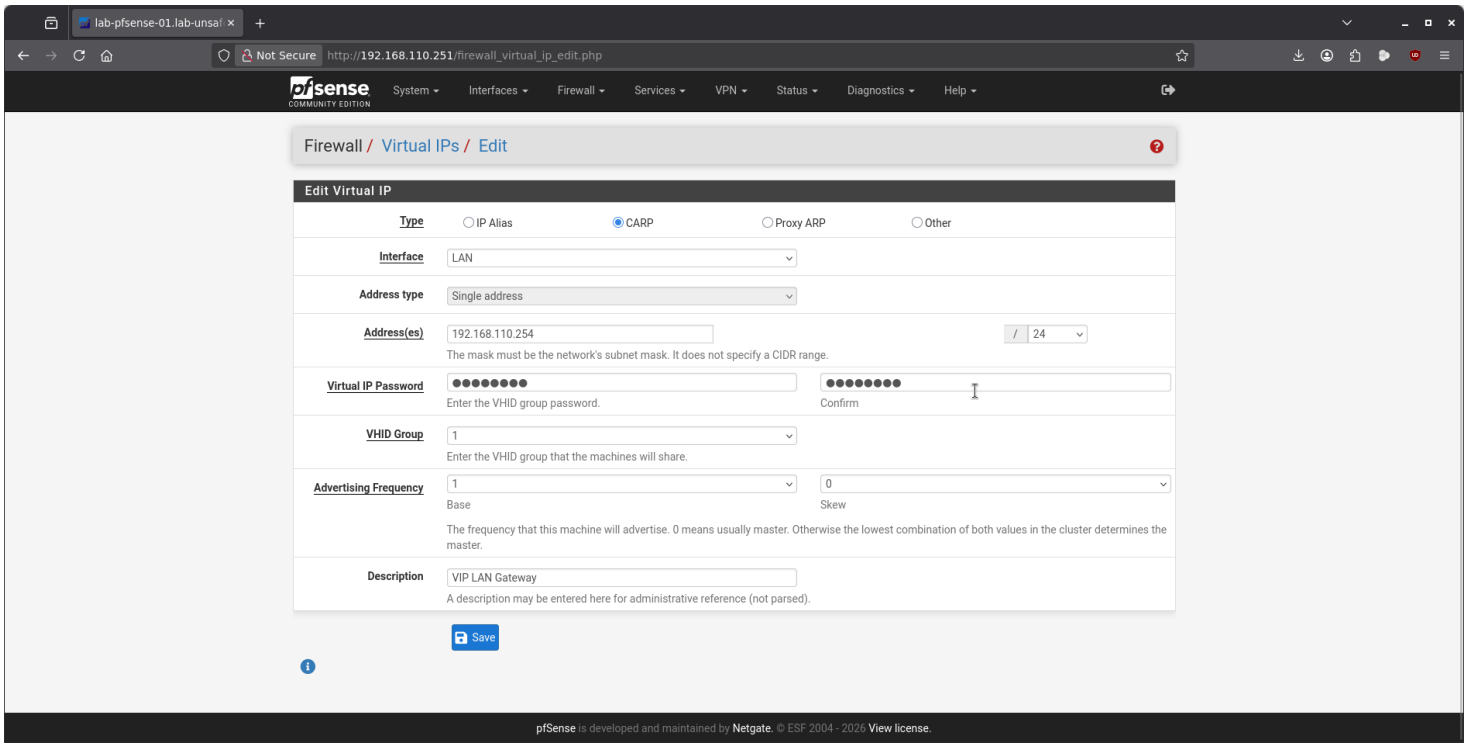
- **Pfsync State Sync :**
  - Cocher Synchronize States.
  - *Interface* : Sélectionner SYNC.
  - *pfsync Peer IP* : 172.16.1.1 (On pointe vers le Maître).

- **XMLRPC Sync :**
  - **NE RIEN CONFIGURER.** (Laisser vide). C'est le Maître qui pousse, l'Esclave ne fait que recevoir.

- **Sauvegarder.**

CRÉATION DES ADRESSES VIRTUELLES (VIP)

L'IP Virtuelle est l'adresse que les clients utiliseront comme passerelle. *Action à effectuer uniquement sur le MASTER. La synchronisation XMLRPC la créera automatiquement sur le Backup.*

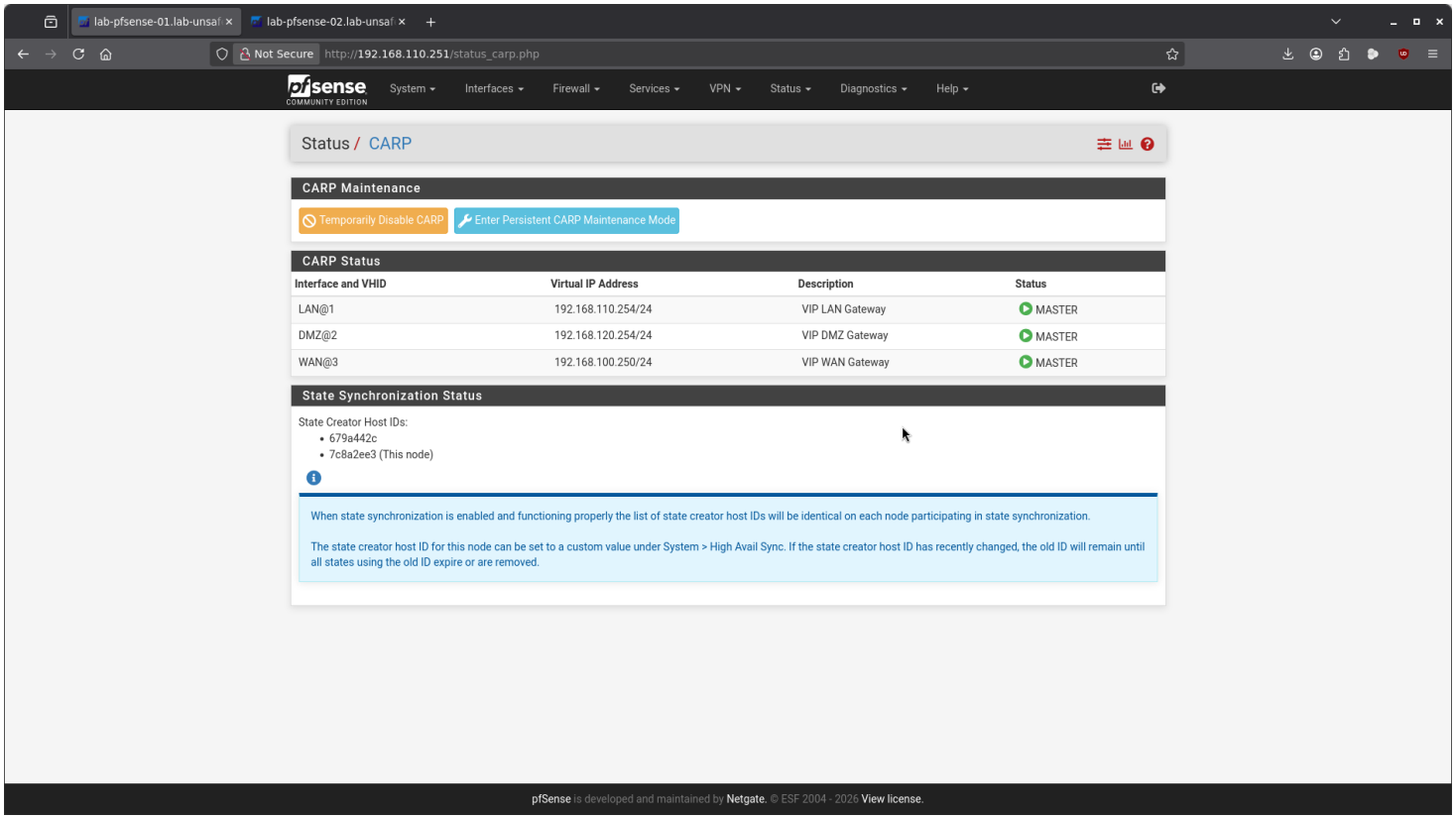


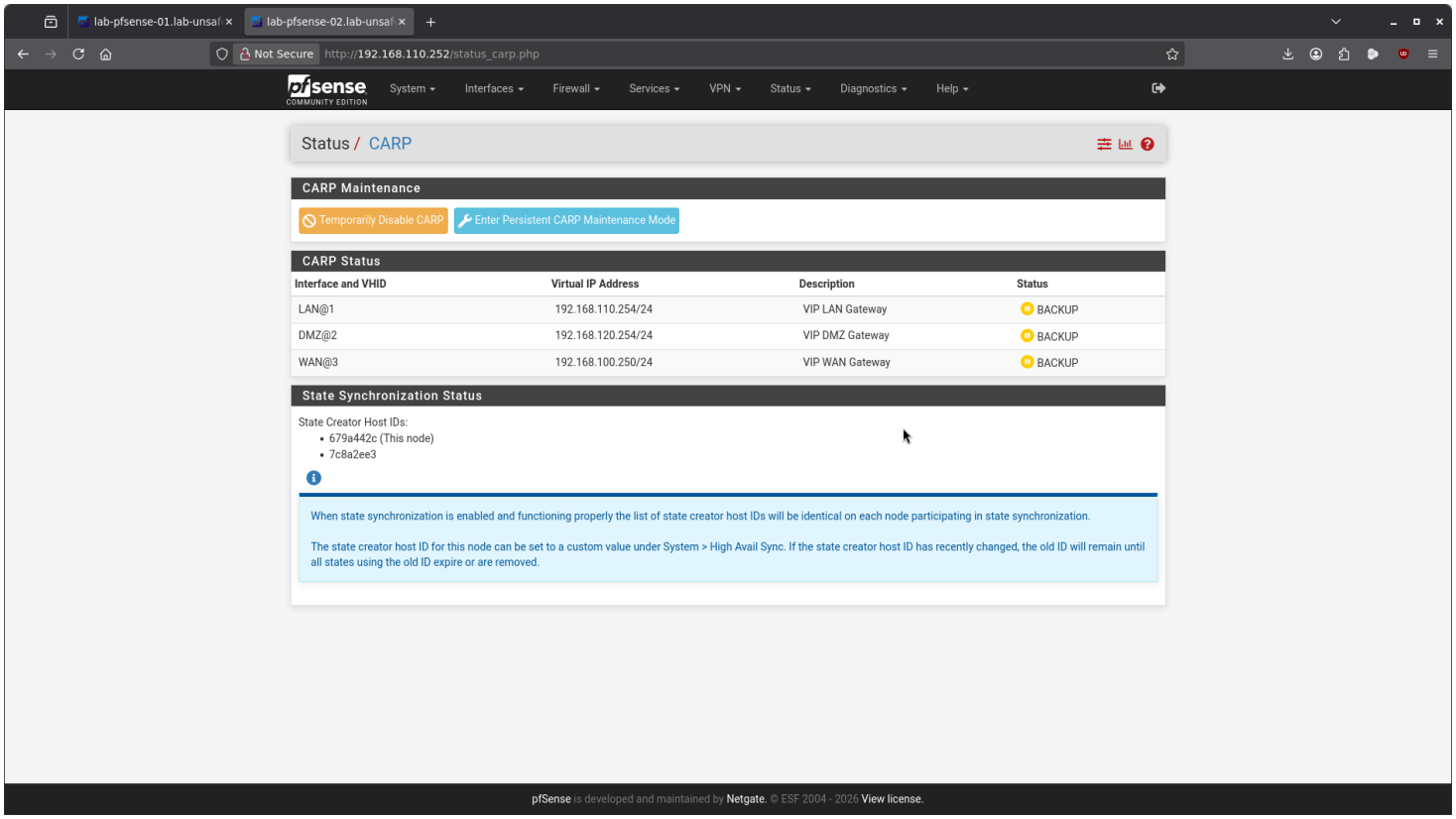
- Aller dans Firewall > Virtual IPs.
  - Cliquer sur Add.
- Configuration (Exemple LAN) :
  - **Type** : CARP.
  - **Interface** : LAN.
  - **Address** : 192.168.110.254 / 24.
  - **Virtual IP Password** : Définir un mot de passe complexe (ex: K33p_It_S3cr3t!).
  - **VHID Group** : 1 (Cet ID doit être unique par interface. Ex: LAN=1, DMZ=2, WAN=3).
  - **Advertising Frequency** :
    - Base : 1
    - Skew : 0 (Le 0 indique "Je suis le Chef Absolu").
  - **Description** : VIP LAN Gateway

Répéter l'opération pour la DMZ et le WAN (avec des VHID différents).

Appliquer les changements.

> **Note** : Après application, vérifier sur le Backup. Le Skew devrait être automatiquement réglé sur 100 (ce qui signifie "Je suis prêt, mais j'attends").





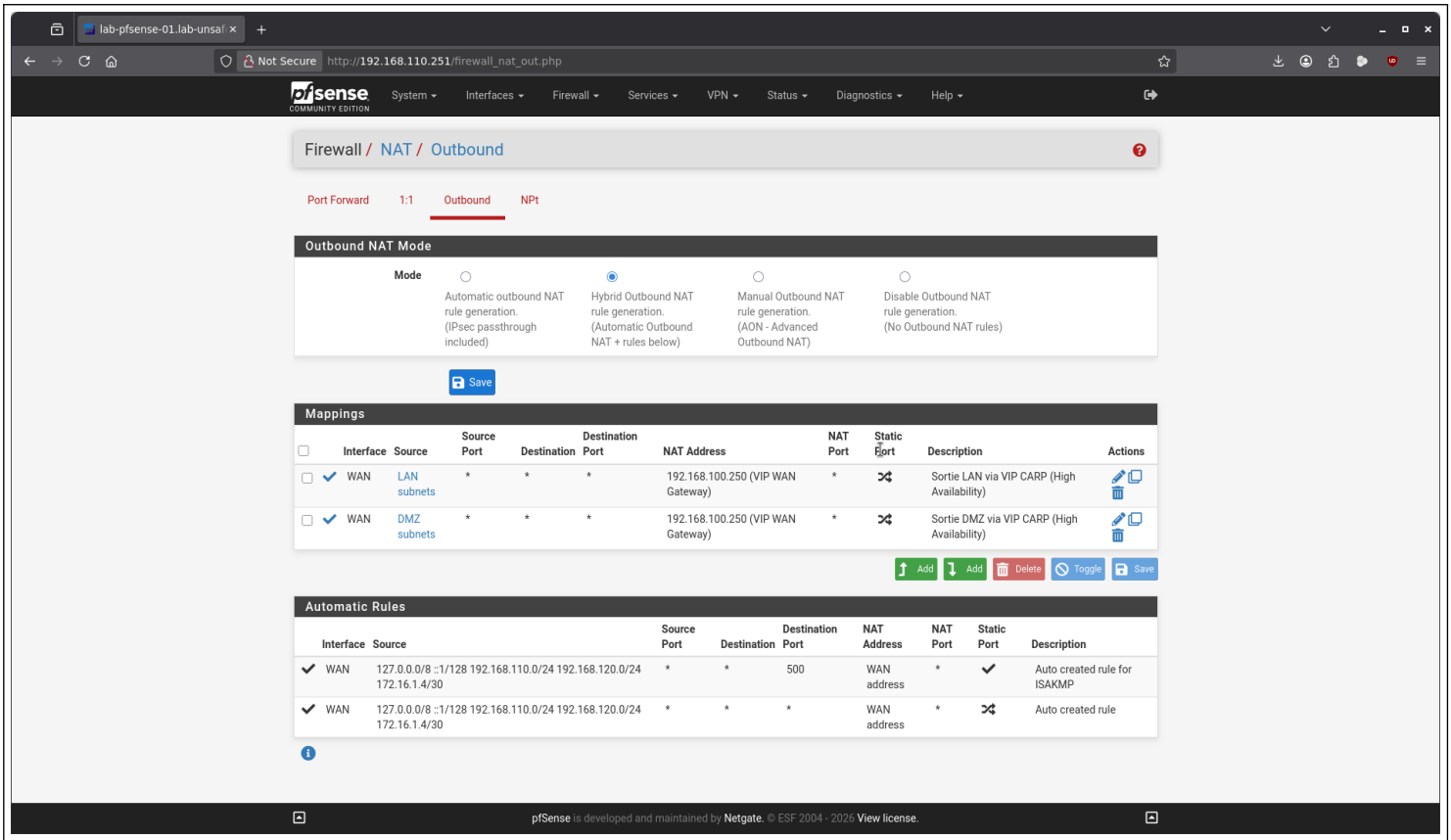
Les captures d'écran ci-dessus illustrent l'état nominal d'un cluster fonctionnel :

1. **Sur le Nœud Primaire (Image 1) :**
   - Toutes les interfaces virtuelles (LAN, WAN, DMZ) affichent le statut **MASTER** (en vert).
   - Cela indique que ce pare-feu possède actuellement les IPs Virtuelles et traite le trafic.
2. **Sur le Nœud Secondaire (Image 2) :**
   - Toutes les interfaces affichent le statut **BACKUP**.
   - Le pare-feu est en écoute passive. Il reçoit bien les annonces du Maître (via le lien XMLRPC/PFSYNC) et sait qu'il doit rester en retrait.

CORRECTION DU NAT SORTANT (OUTBOUND NAT)

Par défaut, pfSense utilise l'adresse IP de l'interface WAN pour sortir sur Internet. En cas de bascule, les connexions seraient coupées car l'IP source changerait. Il faut forcer l'utilisation du VIP WAN.

À faire sur le MAÎTRE uniquement : La synchronisation XMLRPC se chargera de copier la règle sur le Backup.



- Aller dans Firewall > NAT > Outbound.
  - Changer le mode en Hybrid Outbound NAT rule generation.
  - Cliquer sur Save.
- Ajouter une règle (Add) :
  - **Interface :** WAN.
  - **Source :** LAN Subnets.
  - **Translation / Address :** Sélectionner l'adresse VIP WAN (!!! pas l'adresse WAN address !!!).
  - **Description :** Sortie LAN via VIP CARP (High Availability)
- Sauvegarder et Appliquer.

Note : Sans cette étape, lors d'une bascule, les serveurs distants (Internet) continueraient de répondre à l'IP physique de l'ancien Maître (désormais hors ligne), entraînant une rupture de toutes les sessions actives (Téléchargements, SSH, Streaming).

Note de Sécurité (Pourquoi pas "Any" ?) : Bien qu'il soit tentant d'utiliser une source "Any" pour couvrir tous les réseaux internes d'un coup, les bonnes pratiques de sécurité (least Privilege) imposent de créer une règle explicite par sous-réseau (LAN, DMZ). Cela évite de donner l'accès Internet par inadvertance à de futurs VLANs sensibles (ex: Réseau IoT ou Admin) et respecte le principe de "refus par défaut".

REDONDANCE DHCP (FAILOVER)

Il faut s’assurer que le service DHCP continue de fonctionner si le maître tombe, et surtout, garantir que les clients reçoivent bien la **Passerelle Virtuelle (VIP)** et non l'IP physique du serveur.

Actuellement, seul ton Maître donne les clés des chambres (IPs). Si le réceptionniste meurt, l'hôtel est ouvert (CARP), mais plus personne ne peut entrer. Avec le **DHCP Failover**, le Maître et l'Esclave synchronisent leur registre de clients (Database Leases). Si l'un part en pause, l'autre continue de donner les clés.

> **Note :** *Lors de la configuration, s'assurer que le backend DHCP est réglé sur **ISC DHCP**. Le moteur Kea DHCP (plus récent) ne supporte pas encore la synchronisation Failover.*

CONFIGURATION SUR LE MAÎTRE (lab-pfsense-01)

- Aller dans **Services > DHCP Server > LAN**.
- **Gateway :** C'est **CRITIQUE**. Vérifie que le champ Gateway n'est pas vide. Tu **DOIS** entrer l'adresse **VIP LAN** (192.168.110.254).
  - *Pourquoi ?* Si tu laisses vide, pfSense donne sa propre IP physique (.251) comme passerelle. Si le Maître meurt, les clients essaieront toujours de sortir par le .251 (mort) au lieu du VIP.
- **DNS Servers :** Idem, mets le **VIP LAN** (192.168.110.254) si tu utilises le DNS Resolver local.
- Descendre jusqu'à la section **Failover Peer IP**.
  - Saisir l'IP de l'interface **SYNC** du **BACKUP** : 192.168.110.252 (selon ma config).
  - *Note :* On utilise le lien SYNC pour que le trafic de synchro des baux ne pollue pas le LAN.
- **Sauvegarder.**

CONFIGURATION SUR LE BACKUP (lab-pfsense-02)

Attention : XMLRPC ne synchronise PAS toujours parfaitement la config "Failover IP" du DHCP, il faut souvent l'initialiser manuellement.

- Aller dans **Services > DHCP Server > LAN**.
- **Gateway :** Vérifie que c'est bien le **VIP LAN** (.254).
- **Failover Peer IP :** Saisir l'IP de l'interface **SYNC** du **MAÎTRE** : 192.168.110.251
- **Sauvegarder.**

VALIDATION (CHECK STATUS)

- Aller dans **Status > DHCP Leases**.
- Tu devrais voir une ligne "Failover Status".
  - **Maître :** Status normal (State: active).
  - **Backup :** Status normal (State: backup).
- Si tu vois communications-interrupted, c'est que les pare-feux ne se parlent pas sur le port 519/520 (Vérifie tes règles pare-feu sur l'interface SYNC, mais normalement c'est "ANY").

PROTOCOLE DE TEST : "L'INSUBMERSIBLE"

PRÉPARATION (TABLEAU DE BORD)

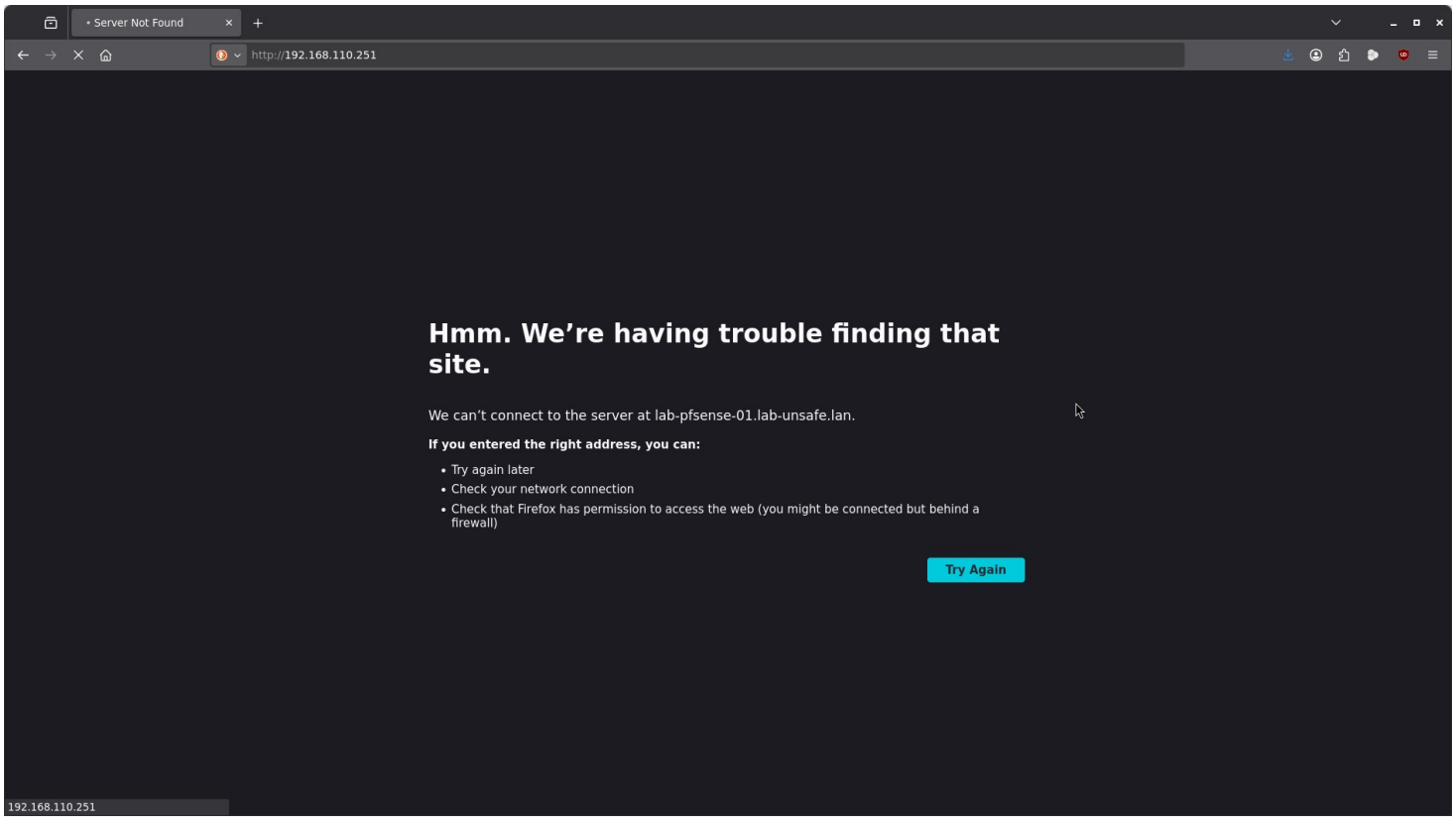
Avant de casser quoi que ce soit, il faut des sondes.

1. **Sur le PC Client (sur le lan) :**
    - Ouvre un terminal (PowerShell ou Bash).
    - Lance un ping infini vers une IP externe stable (Google DNS) : ping 8.8.8.8
2. **Sur le Navigateur (d'un pc sur le lan) :**
    - Lance une vidéo YouTube longue (ou un téléchargement d'ISO linux).
    - Connecte-toi à l'interface Web du **BACKUP (lab-pfsense-02)**.
    - Va dans **Status > CARP**. Garde cette page visible.

L'ACTION (THE KILL SWITCH)

C'est le moment de vérité.

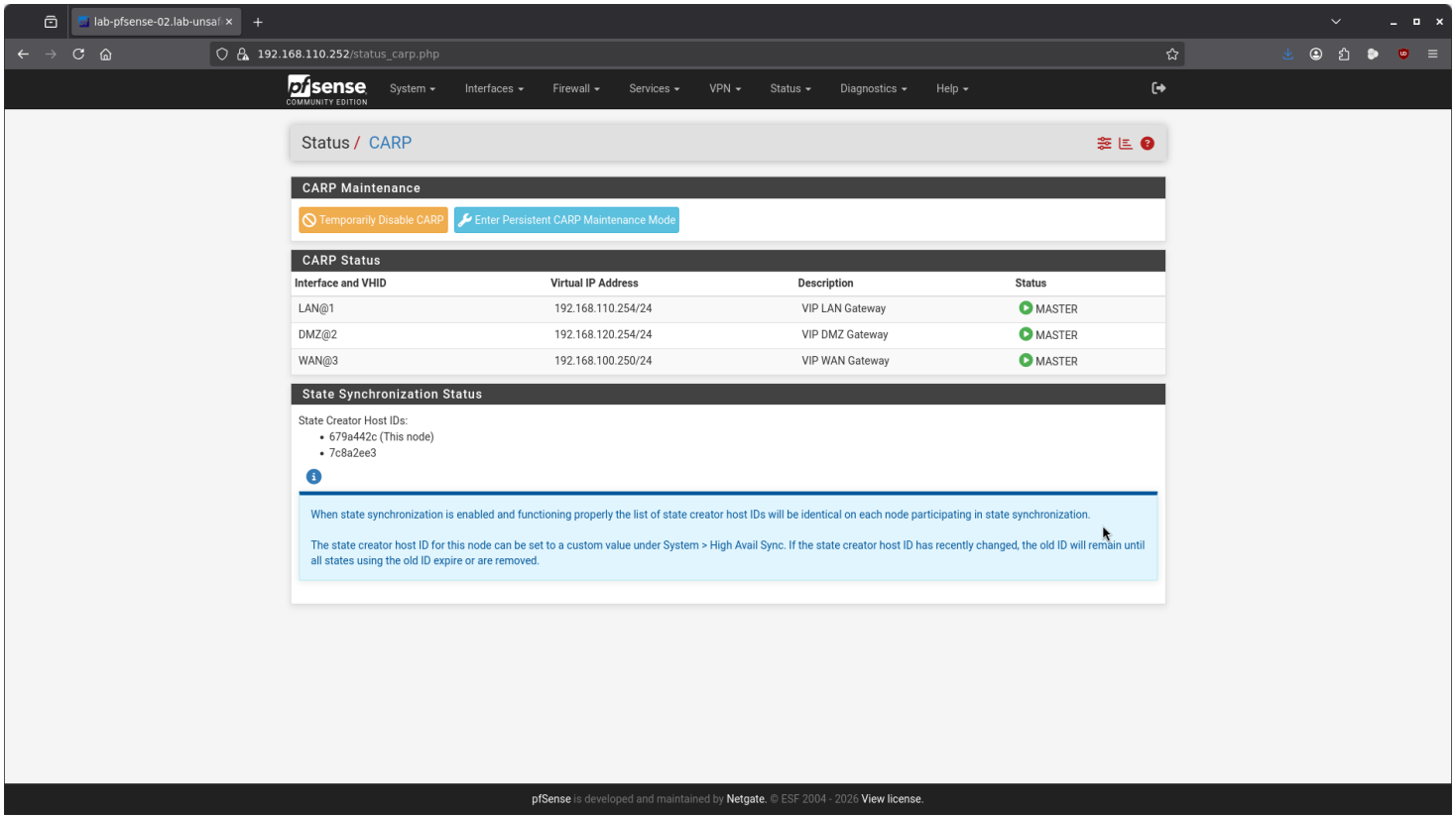
- **Action :** Ne sois pas gentil. Ne fais pas "Redémarrer". Dans ton hyperviseur (KVM/Virt-Manager), fais un clic droit sur la VM lab-pfsense-01 (Master) et choisis **"Force Off"** (Éteindre forcé / Débrancher).



L'OBSERVATION (CE QU'IL DOIT SE PASSER)

Regarde tes sondes immédiatement.

1. **Le Ping :**
    - *Scénario Idéal :* Aucune perte. Les lignes continuent de défiler.
    - *Scénario Réaliste :* "Délai d'attente dépassé" (Request timed out) **une seule fois**, puis ça reprend.
    - *Échec :* Ça ne répond plus du tout.
2. **La Vidéo / Le Téléchargement :**
    - La vidéo ne doit pas bufferiser. Le téléchargement ne doit pas s'arrêter. C'est la preuve que pfsync a bien transféré l'état de la connexion TCP.
3. **L'Interface Web du Backup :**
    - La page **Status > CARP** (rafraîchis si besoin) doit montrer toutes les interfaces en **MASTER**. Le Backup a pris le pouvoir.



LE RETOUR DU ROI (FAILBACK)

On ne laisse pas le Master mort.

- **Action :** Rallume la VM lab-pfsense-01.
- **Observation :**
    - Attends qu'elle boot (c'est le plus long).
    - Dès qu'elle est "Ready", elle va annoncer son Skew de 0 (Priorité absolue).
    - Le lab-pfsense-02 va détecter le chef et repasser gentiment en **BACKUP**.
    - Vérifie tes pings pendant la bascule retour (normalement, c'est transparent).