📜 Guide Complet : Architecture Haute Disponibilité pfSense

Version : 1.0 (Mars 2026)

Infrastructure : Cluster Actif/Passif (Failover) sur Proxmox.

📐 Étape 1 : Préparation Proxmox (Le Matériel Virtuel)

Avant d'allumer les VMs, les "tuyaux" doivent être prêts sur l'hôte.

- **vmbr0 (WAN) :** Connecté à ta Box/Routeur Internet.
- **vmbr1 (LAN) :** Switch virtuel pour tes serveurs (192.168.10.0/24).
- **vmbr2 (OPT1) :** Switch virtuel pour tes clients (192.168.20.0/24).
- **vmbr3 (SYNC) : Crucial.** Un pont isolé sans port physique. C'est le lien privé entre les deux pare-feux.

Configuration des VMs : Les deux VMs pfSense doivent avoir **4 cartes réseau** (virtio) reliées dans l'ordre aux 4 bridges ci-dessus.

🌐 Étape 2 : Adressage des Interfaces (L'Identité Propre)

On configure les adresses "physiques" de chaque machine. **Interdiction d'utiliser le .1 ici.**

pfSense-Master (VM 102)

- **WAN :** 10.113.3.11/16
- **LAN :** 192.168.10.252/24
- **OPT1 :** 192.168.20.252/24
- **SYNC :** 10.0.0.1/30

pfSense-Slave (VM 119)

- **WAN :** 10.113.3.12/16
- **LAN :** 192.168.10.253/24
- **OPT1 :** 192.168.20.253/24
- **SYNC :** 10.0.0.2/30

🔥 Étape 3 : Sécurisation du lien SYNC

Sur les **DEUX** machines, allez dans Firewall > Rules > SYNC :

1. Cliquez sur **Add**.
2. **Protocol :** Any (Indispensable pour laisser passer le protocole PFSYNC).
3. **Source/Destination :** Any.
4. **Save & Apply.**

🔁 Étape 4 : Configuration XMLRPC (La Réplication)

Réglages à faire sur le MASTER UNIQUEMENT (System > High Avail. Sync).

Section : State Synchronization (pfsync)

- **Synchronize states :** ✅ **Coché**. (Partage les sessions actives).
- **Synchronize Interface :** Choisir SYNC.
- **pfsync Synchronize Peer IP :** 10.0.0.1 .

Section : Configuration Synchronization (XMLRPC)

- **Synchronize Config to IP :** 10.0.0.2.
- **Remote System Username :** admin.
- **Remote System Password :** Le mot de passe de l'interface web du Slave.

📋 **Ce qu'il FAUT cocher (Select options to sync) :**

- ✅ **User manager users and groups :** Pour avoir les mêmes admins.
- ✅ **Authentication servers : IMPORTANT.** Pour synchroniser tes réglages **LDAP / Active Directory**. Si tu joins un DNS, le Slave pourra aussi authentifier les users.
- ✅ **Certificate Authorities & Certificates :** Pour le HTTPS.
- ✅ **Firewall Rules :** Le cœur du système.
- ✅ **Firewall Schedules & Aliases :** Pour que tes blocages soient identiques.
- ✅ **NAT Configuration :** Pour que la redirection de ports marche sur les deux.
- ✅ **Static Route :** Si tu as des routes vers d'autres réseaux.
- ✅ **Virtual IPs :** Pour que le Slave "connaisse" les IPs CARP.

💎 Étape 5 : Les IPs Virtuelles CARP (Le costume du Chef)

Sur le MASTER uniquement (Firewall > Virtual IPs). Ces IPs sont celles que les clients utilisent.

Interface	IP Virtuelle	VHID	Password	Rôle
LAN	192.168.10.254	1	PASSWORD	Passerelle Serveurs
OPT1	192.168.20.254	2	PASSWORD	Passerelle Clients

🛠️ Étape 6 : Pourquoi cette configuration est "Blindée" ?

1. **Le Failover DNS/LDAP :** En cochant "Authentication servers", si ton pfSense Master tombe, le Slave connaît déjà ton serveur LDAP. Tes utilisateurs continuent de se connecter sans que le serveur DNS/LDAP ne voie de changement, car il parle à l'IP Virtuelle.
2. **Zéro Split-Brain :** Grâce à l'interface SYNC sur le vmbr3, les deux pare-feux ne se "battent" jamais pour savoir qui est le chef.
3. **Persistance :** ajoutes une règle sur le Master à 14h00, à 14h00 et 1 seconde, le Slave possède la même règle.

🧪 Comment tester ton œuvre ?

1. Va dans Status > CARP. Master doit être en **MASTER**, Slave en **BACKUP**.
2. Lance un ping vers 8.8.8.8 sur un PC client.
3. Éteins le Master.
4. Le Slave devient vert (**MASTER**). Le PC perd maximum 1 seconde de connexion.

Note de fin : pour toute modification future (NAT, Firewall, Users), **travaille toujours sur l'IP du Master (.10)**. Le Slave (.30) est son ombre, il n'agit que si le Master disparaît.