

Procédure Configuration du failover sous PfSense

Table des matières

1	Objectif.....	2
2	Prérequis	3
3	Préparation	4
4	Procédure.....	5
4.1.1	Changement des noms d'interface	5
4.1.2	Configuration XMLRPC Sync.....	6
4.1.3	Configuration des VIPs (CARP)	8
5	Tests de validation.....	9
5.1.1	Vérification du basculement	9
6	Annexes.....	11
6.1	Ressources externes.....	11

1 Objectif

Mettre en place une redondance de pare-feu à l'aide de pfSense en configurant le protocole CARP (Common Address Redundancy Protocol). Cette solution vise à assurer une haute disponibilité du réseau, en garantissant une continuité de service même en cas de défaillance d'un des équipements.

2 Prérequis

Matériels :

- Deux machines physiques ou virtuelles compatibles avec pfSense (x86_64)
- Connexion réseau fiable entre les deux équipements
- Une interface réseau dédiée à la synchronisation (optionnel mais recommandé)

Logiciels et systèmes :

- pfSense (dernière version stable recommandée)
- Navigateur web pour l'administration via l'interface graphique

Réseau :

- Deux adresses IP fixes par interface (LAN/WAN/SYNC) pour chaque nœud
- Une adresse IP virtuelle CARP par interface LAN et WAN
- Accès aux ports suivants :
 - Web UI : HTTP (80), HTTPS (443)
 - CARP : 112 (protocole VRRP, utilisé par CARP)
 - XML-RPC : pour la synchronisation de configuration
- Aucun filtrage entre les interfaces SYNC (autoriser tout le trafic)

3 Préparation

- Plan d'adressage réseau clair, avec au moins :
 - 2 IP fixes LAN (1 par pare-feu)
 - 2 IP fixes WAN (1 par pare-feu)
 - 1 IP CARP LAN (partagée)
 - 1 IP CARP WAN (partagée)
- IP SYNC pour chaque pare-feu (si utilisée)
- Nommer les pare-feux distinctement (ex. pfsense-master et pfsense-backup)
- S'assurer que les ports nécessaires sont ouverts, notamment si un pare-feu en amont est présent
- Prévoir un mot de passe d'administration commun pour la synchronisation XML-RPC
- Préparer les accès au réseau local et à Internet pour tester la continuité de service

4 Procédure

Se connecter aux interfaces web des deux pare-feux

4.1.1 Changement des noms d'interface

Configuration des interfaces sur PfSense-Primary et PfSense-Secondary :

1. Aller dans **Interfaces > Interface Assignements**.
2. **WAN (hn0)** : 172.26.0.154 DHCP (Primary) / 172.26.0.161 DHCP (Secondary)
3. **HA (hn2)** : 10.0.0.1 (Primary) / 10.0.0.2 (Secondary)
4. **DMZ (hn3)** : 192.168.250.252 (Primary) / 192.168.250.253 (Secondary)
5. **LAN (hn4)** : 192.168.1.1 (Primary) / 192.168.1.253 (Secondary)

PfSense-Primary :

Interfaces			
WAN	↑	10Gbase-T <full-duplex>	172.26.0.154
LAN	↑	10Gbase-T <full-duplex>	192.168.1.252
WAN2	↑	10Gbase-T <full-duplex>	n/a
HA	↑	10Gbase-T <full-duplex>	10.0.0.1
DMZ	↑	10Gbase-T <full-duplex>	192.168.250.252

PfSense-Secondary :

Interfaces			
WAN	↑	10Gbase-T <full-duplex>	172.26.0.20
LAN	↑	10Gbase-T <full-duplex>	192.168.1.253
WAN2	↑	10Gbase-T <full-duplex>	n/a
HA	↑	10Gbase-T <full-duplex>	10.0.0.2
DMZ	↑	10Gbase-T <full-duplex>	192.168.250.253

4.1.2 Configuration XMLRPC Sync

Sur PfSense-Primary :

1. Aller dans **System > High Availability Sync**.
2. **Cocher "Synchronize States"** pour permettre la synchronisation des états de connexion.
3. Dans **"Synchronize Interface"**, sélectionner **HA**
4. Entrer l'IP de l'interface HA de **PfSense-Secondary** (10.0.0.2).
5. Renseigner les identifiants des membres en backup (PfSense-Secondary)
6. Définir les paramètres à synchroniser, dans notre cas, tout sélectionner.
7. Enregistrer et appliquer.

State Synchronization Settings (pfsync)	
Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	HA <small>If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.</small>
Filter Host ID	f46f1c8f <small>Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.</small>
pfsync Synchronize Peer IP	10.0.0.2 <small>Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.</small>
Configuration Synchronization Settings (XMLRPC Sync)	
Synchronize Config to IP	10.0.0.2 <small>Enter the IP address of the firewall to which the selected configuration sections should be synchronized. XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!</small>
Remote System Username	admin <small>Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!</small>

Remote System Username	<input type="text" value="admin"/>
Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!	
Remote System Password	<input type="password" value="••••••"/> <input type="password" value="••••••"/>
Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!	
Synchronize admin	<input type="checkbox"/> synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.
Select options to sync	<input checked="" type="checkbox"/> User manager users and groups <input checked="" type="checkbox"/> Authentication servers (e.g. LDAP, RADIUS) <input checked="" type="checkbox"/> Certificate Authorities, Certificates, and Certificate Revocation Lists <input checked="" type="checkbox"/> Firewall rules <input checked="" type="checkbox"/> Firewall schedules <input checked="" type="checkbox"/> Firewall aliases <input checked="" type="checkbox"/> NAT configuration <input checked="" type="checkbox"/> IPsec configuration <input checked="" type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync) <input checked="" type="checkbox"/> DHCP Server settings <input checked="" type="checkbox"/> DHCP Relay settings <input checked="" type="checkbox"/> DHCPv6 Relay settings <input checked="" type="checkbox"/> WoL Server settings <input checked="" type="checkbox"/> Static Route configuration <input checked="" type="checkbox"/> Virtual IPs <input checked="" type="checkbox"/> Traffic Shaper configuration <input checked="" type="checkbox"/> Traffic Shaper Limiters configuration <input checked="" type="checkbox"/> DNS Forwarder and DNS Resolver configurations <input checked="" type="checkbox"/> Captive Portal <input checked="" type="checkbox"/> Toggle All
<input type="button" value="Save"/>	

Sur PfSense-Secondary :

1. Aller dans **System > High Availability Sync**.
2. **Cocher "Synchronize States"** pour permettre la synchronisation des états de connexion.
3. Dans **"Synchronize Interface"**, sélectionner **HA**
4. Entrer l'IP de l'interface HA de **PfSense-Primary** (10.0.0.1).
5. Définir les paramètres à synchroniser, dans notre cas, tout sélectionner.
6. Enregistrer et appliquer.

4.1.3 Configuration des VIPs (CARP)

Pour chaque réseau (**WAN, DMZ, LAN**), on va créer une **IP virtuelle partagée** :

VIP WAN (CARP)

- **PfSense-Primary** → Firewall > Virtual IPs > Add
- **Type** : CARP
- **Interface** : WAN
- **Adresse VIP** : 172.26.0.254/23
- **Virtual CARP ID** : 1
- **Skew** : 0 (Master)
- **Mot de passe** : Définir un mot de passe sécurisé
- **Enregistrer**

VIP LAN (CARP)

- **PfSense-Primary** → Firewall > Virtual IPs > Add
- **Type** : CARP
- **Interface** : LAN
- **Adresse VIP** : 192.168.1.254/24
- **Virtual CARP ID** : 2
- **Skew** : 0 (Master)
- **Mot de passe** : Même que WAN
- **Enregistrer**

VIP DMZ (CARP)

- **PfSense-Primary** → Firewall > Virtual IPs > Add
- **Type** : CARP
- **Interface** : DMZ
- **Adresse VIP** : 192.168.250.254/24
- **Virtual CARP ID** : 3
- **Skew** : 0 (Master)
- **Mot de passe** : Même que WAN
- **Enregistrer**

Les VIPs seront automatiquement répliquées sur **PfSense-Secondary** via **XMLRPC**.

5 Tests de validation

5.1.1 Vérification du basculement

1. **Status > CARP sur PfSense-Primary** : Toutes les VIPs doivent être **MASTER**.

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.1.254/24	LAN virt IP	▶ MASTER
DMZ@2	192.168.250.254/24	DMZ virt IP	▶ MASTER
WAN@3	172.26.1.25/24	WAN virt IP	▶ MASTER

State Synchronization Status	
State Creator Host IDs:	
<ul style="list-style-type: none"> • 52b62caf • f46f1c8f (This node) 	

2. **Status > CARP sur PfSense-Secondary** : Toutes les VIPs doivent être **BACKUP**.

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.1.254/24	LAN virt IP	⏸ BACKUP
DMZ@2	192.168.250.254/24	DMZ virt IP	⏸ BACKUP
WAN@3	172.26.1.25/24	WAN virt IP	⏸ BACKUP

State Synchronization Status	
State Creator Host IDs:	
<ul style="list-style-type: none"> • 52b62caf (This node) • f46f1c8f 	

3. **Débrancher PfSense-Primary** → Vérifier que **PfSense-Secondary** devient **MASTER** et que les IPs restent accessibles.

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.1.254/24	LAN virt IP	▶ MASTER
DMZ@2	192.168.250.254/24	DMZ virt IP	▶ MASTER
WAN@3	172.26.1.25/24	WAN virt IP	▶ MASTER

State Synchronization Status	
State Creator Host IDs:	
<ul style="list-style-type: none"> • 52b62caf (This node) • f46f1c8f 	

Tracert vers CloudFlare DNS (depuis un poste dans le réseau LAN) → Vérifier la continuité du routage.

```
C:\Users\localadmin>tracert 1.1.1.1

Détermination de l'itinéraire vers one.one.one.one [1.1.1.1]
avec un maximum de 30 sauts :

 1  <1 ms  <1 ms  <1 ms  192.168.1.252
 2   1 ms  <1 ms  <1 ms  172.26.1.254
 3   *      *      *      Délai d'attente de la demande dépassé.
 4   1 ms  2 ms   *      10.239.254.2
 5   3 ms  10 ms  2 ms   10.239.254.1
 6   3 ms  2 ms   3 ms   10.243.7.64
 7   1 ms  4 ms   2 ms   46.18.224.50
 8   *      3 ms   7 ms   cpe-et012708.cust.jaguar-network.net [85.31.197.93]
 9   4 ms  3 ms   4 ms   hu0-0-2-1.er02.lyo03.jaguar-network.net [85.31.197.92]
10   3 ms  3 ms   4 ms   one.one.one.one [1.1.1.1]

Itinéraire déterminé.
```

Temps de bascule : La transition entre **PfSense-Primary** et **PfSense-Secondary** s'effectue en quelques secondes.

Résultat : La redondance des routeurs et le **failover** fonctionnent comme prévu, assurant la continuité des services réseau.

6 Annexes

6.1 Ressources externes

[1]

M. Dorigny, « Fail-Over PfSense via CARP et pfsync | pfSense | IT-Connect ». Consulté le: 21 mai 2025. [En ligne]. Disponible sur: <https://www.it-connect.fr/fail-over-pfsense-via-carp-et-pfsync/>

[2]

Guillaume, « [pfSense] Configurer un cluster de 2 pfSense redondants (failover) - Provya ». Consulté le: 21 mai 2025. [En ligne]. Disponible sur: <https://provya.net/?d=2016/10/02/07/48/16-pfsense-configurer-un-cluster-de-2-pfsense-redondants-failover>

[3]

« High Availability Configuration Example | pfSense Documentation ». Consulté le: 21 mai 2025. [En ligne]. Disponible sur: <https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html>

[4]

« TUTORIEL-6-HAUTE-DISPONIBILITE-AVEC-PFSENSE ». Consulté le: 21 mai 2025. [En ligne]. Disponible sur: <https://tutos-info.fr/wp-content/uploads/2024/02/TUTORIEL-6-HAUTE-DISPONIBILITE-AVEC-PFSENSE.pdf>