

## Création d'un cluster PfSense

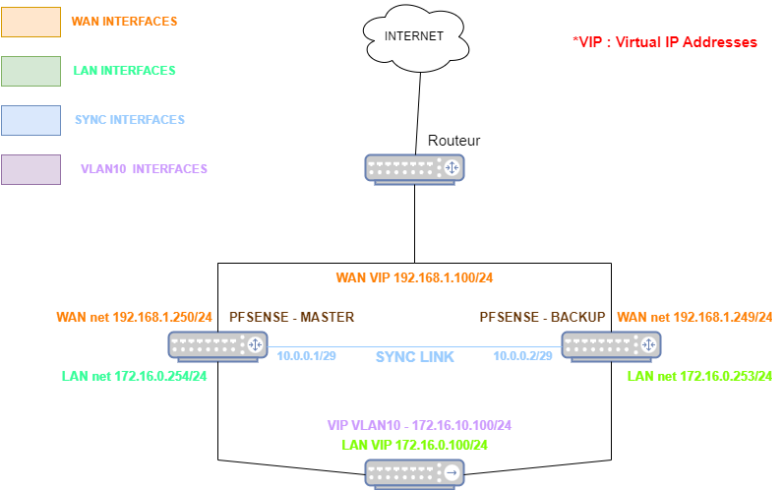
Version de Proxmox : 8.1.3  
Version de PfSense : 2.6.0

1 – Infrastructure de démonstration .....	1
2 – Prérequis .....	2
3 – Création de la synchronisation .....	3
4 – Création des adresses CARP (VIP) .....	5
5 – Création des règles NAT .....	6
6 – Configuration du service DHCP .....	7
7 – Test du cluster .....	8

*Pour cette procédure, je pars du principe que vous avez déjà deux PfSense avec au moins les configurations minimales LAN & WAN.*

### 1 – Infrastructure de démonstration

Ci-dessous, vous trouverez le schéma réseau afin d'avoir une bonne compréhension de la configuration :




















Les adresses VIP (Virtual IP Adresses) sont les adresses IP qui rassemble les deux PfSense et donc identifient le cluster.

Il y a un PfSense maître, qui gère toute la configuration et un PfSense backup qui lui va se synchroniser avec le PfSense maître.


















## 2 – Prérequis

Afin que le cluster fonctionne de manière optimale, il vous faudra deux PfSense possédant les mêmes interfaces réseaux. Vous trouverez ci-dessous un exemple de configuration de mes deux PfSense.

### PFSense MASTER :

Interfaces   			
 WAN		10Gbase-T <full-duplex>	192.168.1.250
 LAN		10Gbase-T <full-duplex>	172.16.0.254
 SYNC		10Gbase-T <full-duplex>	10.0.0.1
 AVLANSRV10		10Gbase-T <full-duplex>	172.16.10.254
 AVLANDSI20		10Gbase-T <full-duplex>	172.16.20.254
 AVLANADM30		10Gbase-T <full-duplex>	172.16.30.254
 AVLANSISR40		10Gbase-T <full-duplex>	172.16.40.254





### PFSense BACKUP :


Interfaces   			
 WAN		10Gbase-T <full-duplex>	192.168.1.249
 LAN		10Gbase-T <full-duplex>	172.16.0.253
 SYNC		10Gbase-T <full-duplex>	10.0.0.2
 AVLANSRV10		10Gbase-T <full-duplex>	172.16.10.253
 AVLANDSI20		10Gbase-T <full-duplex>	172.16.20.253
 AVLANADM30		10Gbase-T <full-duplex>	172.16.30.253
 AVLANSISR40		10Gbase-T <full-duplex>	172.16.40.253

Assurez-vous d'avoir également une règle de pare-feu qui autorise la communication sur vos interfaces


FloatingWANLANSYNCAVLANSRV10AVLANDSI20AVLANADM30AVLANSISR40

Rules (Drag to Change Order)


<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>




Add




Add




Delete




Toggle



Copy



Save



Separator

### 3 – Création de la synchronisation

Dans cette partie nous allons mettre en place la synchronisation du PfSense maître vers le PfSense backup (se référer au schéma réseau).

Sur le PfSense maître, rendez-vous dans **System -> High Availability** et renseignez les informations suivantes

**State Synchronization Settings (pfsync)**

**Synchronize states** ☒ 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**  Utilisez bien l'interface SYNC dédiée à la synchronisation  
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.

---

**Configuration Synchronization Settings (XMLRPC Sync)**

**Synchronize Config to IP**  IP du PfSense Backup  
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!

**Remote System Username**  Identifiants du PfSense Backup  
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**   Confirm  
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!

☒ Virtual IPs  
☒ Traffic Shaper configuration  
☒ Traffic Shaper Limiters configuration  
☒ DNS Forwarder and DNS Resolver configurations  
☒ Captive Portal  
☒ Toggle All

Activer Windows

Nous allons maintenant créer un utilisateur dédié pour la synchronisation des PfSense, de ce fait le compte admin ne sera pas utilisé.

Allez dans **System -> User Manager** et cliquez sur **Add**

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 admin	System Administrator		admins	
					<div><div> Add</div><div> Delete</div></div>

Renseignez des identifiants et sauvegardez

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="syncuser"/>
Password	<input type="password" value="*****"/> <input type="password" value="*****"/>

Retournez maintenant modifiez votre utilisateur pour ajouter les droits de synchronisation

Users Groups Settings Authentication Servers

### Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	syncuser		✓		

[+ Add](#) [Delete](#)

### Effective Privileges

Inherited from	Name	Description	Action
			<a href="#">+ Add</a>

### User Privileges

User: syncuser

Assigned privileges:

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted sc
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin

Une fois fait, vous devriez vous retrouver avec la ligne suivante dans les privilèges

### Effective Privileges

Inherited from	Name	Description	Action
	System - HA node sync	Allow access to authenticate this user for HA sync via XMLRPC (admin privilege)	

Security notice: This user effectively has administrator-level access

[+ Add](#)

Vous pouvez ainsi sauvegardez vos modifications.

On va maintenant modifier l'utilisateur admin pour la synchronisation par celui que nous venons de créer.

Retournez dans **System -> High Availability** et modifiez les identifiants

La synchronisation est maintenant terminée. Cela signifie que les modifications que vous ferez sur le PfSense maître seront automatiquement répliquées sur le PfSense backup.

## 4 – Création des adresses CARP (VIP)







Nous allons dans cette section, créer les adresses virtuelles qui serviront à identifier le cluster de PfSense.

Rendez-vous dans **Firewall -> Virtual IPs** puis cliquez sur **Add**

Il faudra faire cette étape pour chaque interface.

Ajoutez les informations suivantes :

Une fois la configuration effectuée pour chaque interface, vous devriez vous retrouver avec quelque chose comme cela

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.1.100/24 (vhid: 1)	WAN	CARP	VIP WAN	 
172.16.0.100/24 (vhid: 2)	LAN	CARP	VIP LAN	 
172.16.10.100/24 (vhid: 3)	AVLANSRV10	CARP	VIP AVLAN10	 

## 5 – Création des règles NAT

Nous allons maintenant devoir créer une règle NAT pour que le trafic soit redirigé vers le VIP WAN.

Cette opération sera à répéter pour toutes vos interfaces (LAN & VLANs).


Rendez-vous dans **Firewall -> NAT -> Outbound** et activez le mode **Hybrid Outbound**

Port Forward 1:1 Outbound NPT

### Outbound NAT Mode






Mode

☐ Automatic outbound NAT rule generation. (IPsec passthrough included)
 ☒ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
 ☐ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
 ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

 Save

Nous allons maintenant ajoutez notre règle

### Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div>  Add            Add            Delete            Toggle            Save         </div>									

### Edit Advanced Outbound NAT Entry

☐ Disabled ☐ Disable this rule

**Do not NAT** ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required.

**Interface** WAN L'interface à utiliser  
 The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** any  
 Choose which protocol this rule should match. In most cases "any" is specified. L'adresse réseau locale, ici le LAN

**Source** Network 172.16.0.0 / 24   
 Type Source network for the outbound NAT mapping. Port or Range

**Destination** Any  / 24   
 Type Destination network for the outbound NAT mapping. Port or Range

☐ Not  
 Invert the sense of the destination match.

Activier Windows  
 Accédez aux paramètres pour active

**Translation**

**Address** 192.168.1.100 (VIP WAN)

Connections matching this rule will be mapped to the specified **Address**.  
The **Address** can be an Interface, a Host-type Alias, or a [Virtual IP](#) address.

**Port or Range**  ☐ Static Port

Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by \*.\*.  
Leave blank when **Static Port** is checked.

Activer Windows  
Accédez aux paramètres pour activer Windows

Après avoir répété l'opération pour vos LANs et VLANs, vous devriez vous retrouver avec plusieurs règles, une pour chaque interface

Mappings										
<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	✓ WAN	172.16.0.0/24	*	*	*	192.168.1.100	*	<input checked="" type="checkbox"/>	LAN Outbound	
<input type="checkbox"/>	✓ AVLANSRV10	172.16.10.0/24	*	*	*	192.168.1.100	*	<input checked="" type="checkbox"/>	VLAN10 Outbound	

Add
 Add
 Delete
 Toggle
 Save

## 6 – Configuration du service DHCP

Dans notre cas, le DHCP est fourni par PfSense. Nous allons donc modifier la configuration de sorte que le DHCP puisse être fourni dans le cas où le DHCP du PfSense maître tomberait hors service.

Rendez-vous dans **Services -> DHCP Server** et sélectionnez votre LAN

WAN
LAN
SYNC
AVLANSRV10
AVLANDSI20
AVLANADM30
AVLANSISR40

**General Options**

**Enable** ☒ Enable DHCP server on LAN interface

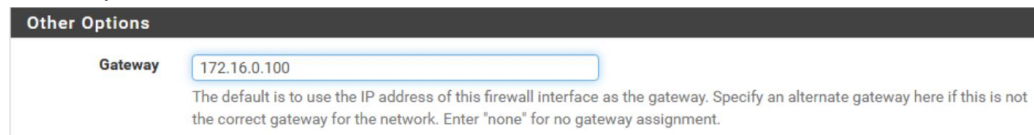
**BOOTP** ☐ Ignore BOOTP queries

Définissez votre range DHCP

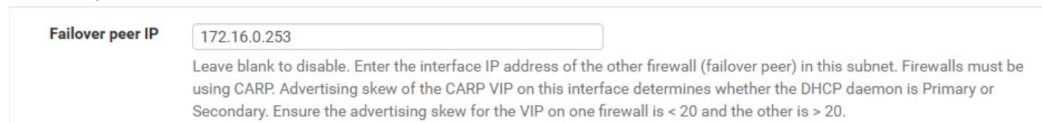
**Range**

From To

Dans l'option **Gateway**, il faudra renseigner la VIP du LAN (référez-vous au schéma si besoin)



Dans l'option **Failover peer IP**, renseignez l'adresse IP physique LAN du PfSense Backup



Répétez ensuite l'opération pour vos autres interfaces, en faisant correspondre les adresses.

Vous avez d'ailleurs pu remarquer que nous n'avons rien configuré sur le PfSense Backup. Cela s'est fait automatiquement grâce à la synchronisation.

## 7 – Test du cluster

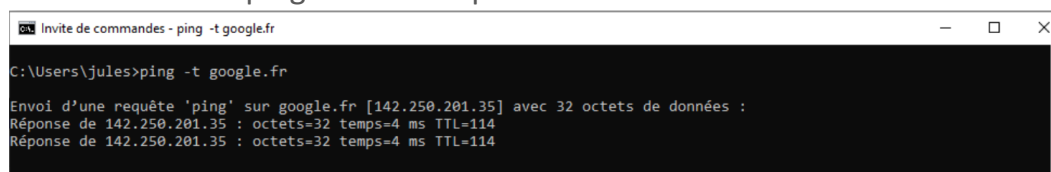
Nous allons maintenant nous assurer que notre cluster est bien fonctionnel. Pour ce faire nous arrêterons le PfSense maître et vérifierons que notre machine a toujours un accès réseau.

Voici donc ma configuration IP, je suis dans le LAN

```
Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . : jumas.local
Adresse IPv6 de liaison locale. . . . : fe80::82b5:95f1:4c10:8308%10
Adresse IPv4. . . . . : 172.16.0.30
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 172.16.0.100
```

Je vais lancer un ping en continu pour vérifier la connectivité



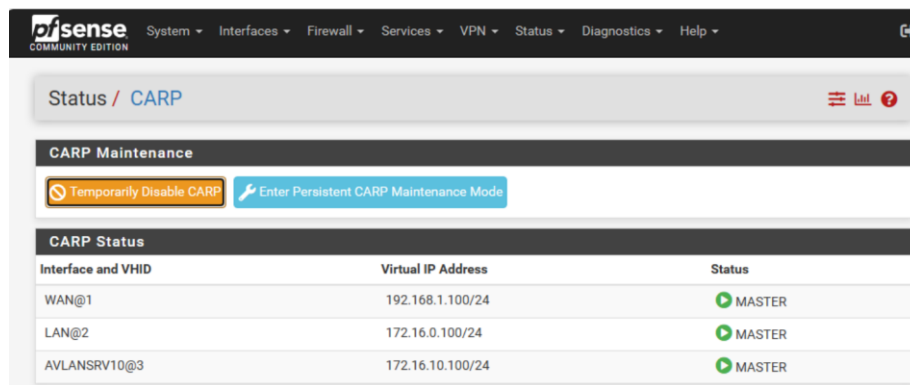


On va maintenant arrêter le PfSense maître et vérifier notre ping

```
Réponse de 142.250.201.35 : octets=32 temps=3 ms TTL=114
Réponse de 142.250.201.35 : octets=32 temps=3 ms TTL=114
Délai d'attente de la demande dépassé.
Réponse de 142.250.201.35 : octets=32 temps=4 ms TTL=114
Réponse de 142.250.201.35 : octets=32 temps=4 ms TTL=114
Réponse de 142.250.201.35 : octets=32 temps=5 ms TTL=114
Réponse de 142.250.201.35 : octets=32 temps=3 ms TTL=114
Réponse de 142.250.201.35 : octets=32 temps=3 ms TTL=114
```

Comme vous pouvez le voir je n'ai perdu qu'une seule requête !

Pendant que le PfSense maître est arrêté, c'est le PfSense Backup qui devient le maître.



Lorsque le PfSense maître sera à nouveau opérationnel, il deviendra à nouveau maître, automatiquement sans configuration requise.

Pour vos serveurs avec une adresse IP fixe, n'oubliez pas de mettre l'adresse IP virtuelle du réseau concerné en tant que passerelle !

**Fin de la procédure.**