

CARP Failover sur pfSense

Configuration d'un CARP
entre 2 pfSense

EHRET Louis

Table des matières

1. Configuration des postes.....	2
2. Création des IP virtuelles sur le 1 ^{er} pfsense	3
2.1 CARP WAN.....	3
2.2 CARP LAN	3
2.3 CARP DMZ.....	4
3. Configuration des IP virtuelles pour le 2 ^{ème} pfsense.....	4
4. Tests d'intégration du CARP	5

1. Configuration des postes

SECCIV-RTE-01

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.10.0
VMnet1	Custom	-	-	-	192.168.100.0
VMnet2	Custom	-	-	-	192.168.200.0
VMnet3	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz	-	-	-

```

WAN (wan)    -> em0    -> v4: 192.168.10.11/24
LAN (lan)    -> em1    -> v4: 192.168.100.251/24
DMZ (opt1)   -> em2    -> v4: 192.168.200.251/24
            
```

SECCIV-RTE-02

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.10.0
VMnet1	Custom	-	-	-	192.168.100.0
VMnet2	Custom	-	-	-	192.168.200.0
VMnet3	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz	-	-	-

```

WAN (wan)    -> em0    -> v4: 192.168.10.12/24
LAN (lan)    -> em1    -> v4: 192.168.100.252/24
DMZ (opt1)   -> em2    -> v4: 192.168.200.252/24
            
```

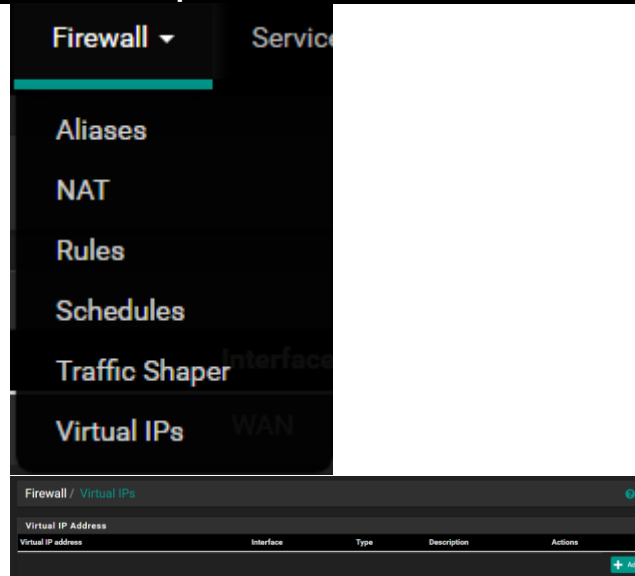
« On appelle un groupe d'hôtes utilisant CARP un « groupe de redondance ». Le groupe de redondance se voit attribuer une adresse IP partagée entre les membres du groupe. Au sein de ce groupe, un hôte est désigné comme « maître », les autres sont appelés « esclaves ». L'hôte maître est celui qui « prend » l'adresse IP partagée. Il répond à tout trafic ou requête ARP à destination de cette adresse. Chaque hôte doit avoir une seconde adresse IP unique. Chaque hôte peut appartenir à plusieurs groupes de redondance. »

2. Création des IP virtuelles sur le 1^{er} pfSense

Sur le premier pare-feu, j'accède à Firewall -> Virtual IPs.

Nous allons faire des IP virtuelles que les 2 postes vont pouvoir conjointement utiliser.

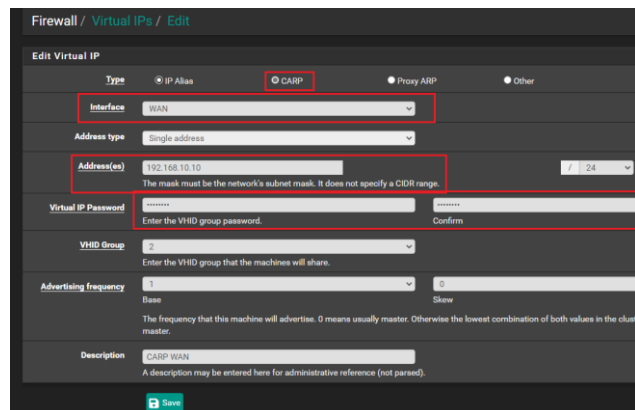
Nous pouvons cliquer sur add.



2.1 CARP WAN

On va configurer le CARP pour le WAN.

Sélectionner WAN, avec une adresse IP range, la notre c'est 192.168.10.10 avec le mot de passe. De préférence mettre le même sur chaque interface que nous allons créer.



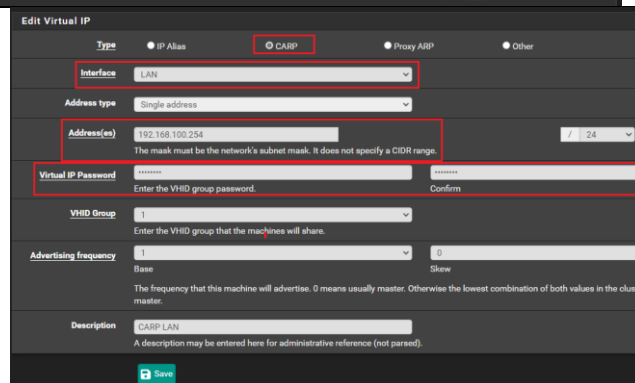
Virtual IP address	Interface	Type	Description	Actions
192.168.10.10/24 (vhid: 2)	WAN	CARP	CARP WAN	

2.2 CARP LAN

Cliquer à nouveau sur add et sélectionner cette fois l'interface LAN

Renseigner l'adresse 192.168.100.254, qui est notre réseau LAN commun.

Indiquer le mot de passe, et le groupe aussi de préférence.



Virtual IP address	Interface	Type	Description	Actions
192.168.100.254/24 (vhid: 1)	LAN	CARP	CARP LAN	

2.3 CARP DMZ

Cliquer à nouveau sur add et sélectionner cette fois l'interface DMZ, car nous allons également configurer Le CARP pour notre DMZ

Renseigner l'adresse 192.168.200.254, qui est notre réseau DMZ commun qui va nous permettre de le faire marcher.

Indiquer le mot de passe, et le groupe aussi de préférence.

192.168.200.254/24 (vhid: 3) DMZ CARP CARP DMZ

Status / CARP

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
WAN@2	192.168.10.10/24	MASTER
LAN@1	192.168.100.254/24	MASTER
DMZ@3	192.168.200.254/24	MASTER
WAN@4	192.168.1.0/32	MASTER

pfSync Nodes

```

pfSync nodes:
8e8c222c
25c95cbb
60d4688b
695b6ecb
a25257eb
c22b6550
cd6d1531
    
```

Nous avons configuré le CARP pour le premier pfsense. On voit bien que le status est en master, car pour le moment nous n'avons qu'un seul pfsense dans le carp.

On peut effectuer un reboot pour enregistrer les éléments ajoutés avec Diagnostics -> Reboot

3. Configuration des IP virtuelles pour le 2^{ème} pfsense

Firewall / Virtual IPs

Virtual IP address	Interface	Type	Description	Actions
192.168.10.10/24 (vhid: 2)	WAN	CARP	CARP WAN	
192.168.100.254/24 (vhid: 1)	LAN	CARP	CARP LAN	
192.168.200.254/24 (vhid: 3)	DMZ	CARP	CARP DMZ	
192.168.1.0/32 (vhid: 4)	WAN	CARP	CARP WAN2	

[+ Add](#)

Réeffectuer la configuration sur le deuxième pfsense avec toutes les informations similaires, en miroir, comme on a fait plus haut. Redémarrer.

4. Tests d'intégration du CARP

The screenshots show the CARP configuration page in pfSense. The left screenshot shows the first node in MASTER status for all interfaces (WAN@2, LAN@1, DMZ@3, WAN@4). The right screenshot shows the second node in BACKUP status for all interfaces. Both screenshots show identical pfSync nodes.

On remarque clairement que nos 2 CARP fonctionnent. On peut le voir car le premier pfsense est en MASTER, donc notre CARP fonctionne sur le premier, et le deuxième est en BACKUP, ce qui veut dire que si le premier pfsense s'arrête, le deuxième obtient le status MASTER ! C'est donc une haute disponibilité !

Les pfsync nodes aussi nous montrent cela, ils sont identiques, ils ont les mêmes informations.

<pre>C:\Users\Administrateur>ping 192.168.10.10 Envoi d'une requête 'Ping' 192.168.10.10 avec 32 octets de données : Réponse de 192.168.10.10 : octets=32 temps<1ms TTL=64 Réponse de 192.168.10.10 : octets=32 temps<1ms TTL=64 Réponse de 192.168.10.10 : octets=32 temps<1ms TTL=64 C:\Users\Administrateur>ping 192.168.100.254 Envoi d'une requête 'Ping' 192.168.100.254 avec 32 octets de données : Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64 Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64 Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64 Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64 C:\Users\Administrateur>PING 192.168.200.254 Envoi d'une requête 'Ping' 192.168.200.254 avec 32 octets de données : Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64 Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64 Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64 Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64</pre>	<p>Si on ping les adresses des CARP, on trouve bien tout, pour le WAN,</p> <p>Le LAN,</p> <p>La DMZ.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------