

Haute Disponibilité avec deux pare-feu pfSense

I. Contexte

Dans le cadre de la sécurisation et de la continuité d'accès à un réseau informatique, la mise en place d'un système de haute disponibilité à l'aide de deux pare-feux configurés avec pfSense permet d'assurer un service ininterrompu. Ce dispositif repose sur un principe de redondance : si le premier pare-feu rencontre un dysfonctionnement, le second prend automatiquement le relais, sans interruption pour les utilisateurs. Cette approche garantit une meilleure fiabilité du réseau, limite les risques de coupure, et contribue à la sécurité et à la stabilité de l'infrastructure.

II. Prérequis

- Deux routeurs pfSense avec minimum trois cartes réseaux chacun.
- Un accès internet.

III. Configurations réseaux des pfSense

A. Configuration réseau pfSense 1

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on PFS1-M2L ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.67.128/24  
LAN (lan)      -> em1      -> v4: 10.75.23.1/24  
OPT1 (opt1)    -> em2      -> v4: 10.75.19.1/30
```

1. La première carte réseau est celle du WAN qui permettra l'accès à internet
2. La deuxième est configurée en tant que passerelle du LAN
3. La troisième servira de connexion directe entre les deux pfSense, avec un masque en /30 pour n'autoriser uniquement que ces dernières dans le réseau.

B. Configuration réseau pfSense 2

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on PFS2-M2L ***

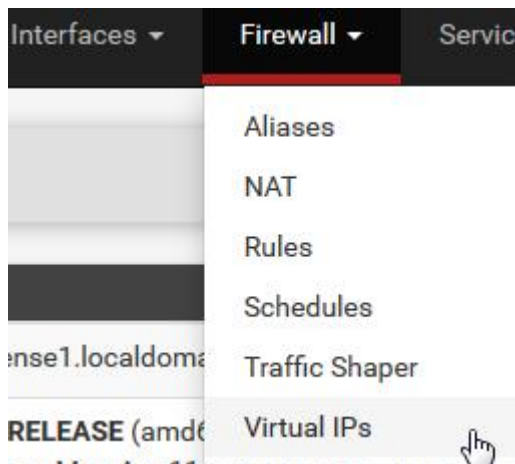
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.67.135/24
LAN (lan)      -> em1      -> v4: 10.75.23.2/24
OPT1 (opt1)    -> em2      -> v4: 10.75.19.2/30
```

Comme pour la première pfSense, nous configurons les différentes cartes réseaux.

IV. Mise en place de la Haute Disponibilité

1. Configurer les adresses IP virtuelles

Pour assurer le fonctionnement en haute disponibilité, chaque serveur pfSense nécessitera une adresse IP dédiée sur son interface physique. De plus, une adresse IP virtuelle unique sera configurée et partagée entre les deux serveurs. Ainsi, chaque réseau concerné nécessitera l'attribution de trois adresses IP : une pour chaque serveur physique et une adresse virtuelle pour la redondance.



- **Interface :** l'interface sur laquelle la VIP doit être configurée. Ici, on configure la VIP sur l'interface LAN.
- **Adresse(s) :** Nous utiliserons l'adresse VIP 10.75.23.3 avec un masque de sous-réseau /24 pour l'interface.
- **Virtual IP Password :** Un mot de passe de sécurité sera défini pour authentifier les communications entre les deux serveurs pfSense partageant la VIP. Ce même mot de passe devra être configuré sur le serveur pfSense secondaire.

- **VHID Group** : Nous changeons l'identifiant de groupe virtuel (VHID) par défaut et nous mettons l'ID "2" pour identifier ce groupe de VIP.
- **Advertising Frequency** : Pour déterminer le rôle des serveurs, le champ "Skew" sera réglé à 0 sur le serveur primaire (master), et une valeur supérieure sur le serveur secondaire (slave). La valeur "Base", qui définit le délai en secondes avant de considérer un hôte comme inactif, sera laissée à sa valeur par défaut de 1 seconde.

Exemple de résultat obtenu :

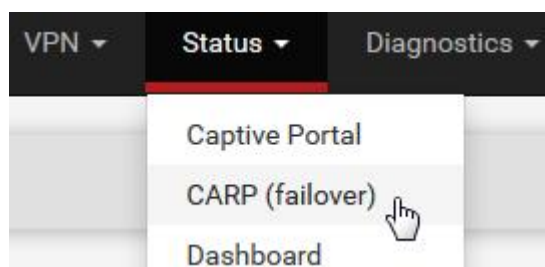
The screenshot shows the 'Edit Virtual IP' page in the pfSense web interface. The breadcrumb trail is 'Firewall / Virtual IPs / Edit'. The form is titled 'Edit Virtual IP' and contains the following fields:

- Type**: Radio buttons for IP Alias, **CARP** (selected), Proxy ARP, and Other.
- Interface**: A dropdown menu showing 'LAN'.
- Address type**: A dropdown menu showing 'Single address'.
- Address(es)**: A text input field containing '10.75.23.3' and a mask dropdown set to '24'. A note below states: 'The mask must be the network's subnet mask. It does not specify a CIDR range.'
- Virtual IP Password**: Two password input fields (one masked with dots) with a 'Confirm' label.
- VHID Group**: A dropdown menu showing '2'. A note below states: 'Enter the VHID group that the machines will share.'
- Advertising frequency**: Two dropdown menus. The first is 'Base' set to '1'. The second is 'Skew' set to '0'. A note below states: 'The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.'
- Description**: A text input field containing 'CARP LAN'. A note below states: 'A description may be entered here for administrative reference (not parsed).'

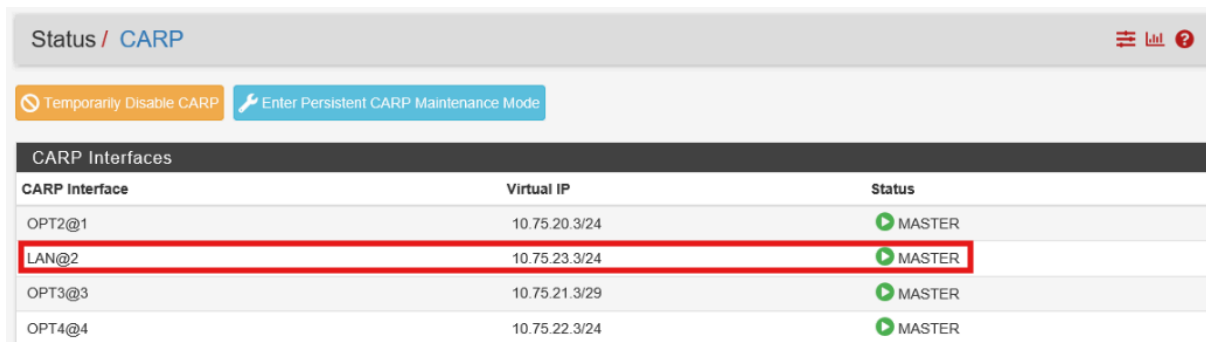
A blue 'Save' button is located at the bottom of the form.

Pour finaliser la configuration de la haute disponibilité, nous allons répliquer les mêmes étapes sur l'interface LAN du serveur pfSense secondaire (pfSense 2). Une attention particulière sera portée au champ "Skew", dont la valeur devra être impérativement réglée à 1 sur ce serveur.

Une fois cette configuration terminée, l'état de l'adresse IP virtuelle et le statut du basculement (CARP) pourront être consultés et vérifiés à tout moment via le menu "Status" puis "CARP (failover)" de l'interface web de pfSense.



Dans le cas présent, l'adresse VIP créée a bien le statut "master" sur le pfSense 1 :



The screenshot shows the 'Status / CARP' page in pfSense. At the top, there are two buttons: 'Temporarily Disable CARP' (orange) and 'Enter Persistent CARP Maintenance Mode' (blue). Below these is a table titled 'CARP Interfaces'. The table has three columns: 'CARP Interface', 'Virtual IP', and 'Status'. The row for 'LAN@2' is highlighted with a red box, and its status is 'MASTER'.

CARP Interface	Virtual IP	Status
OPT2@1	10.75.20.3/24	MASTER
LAN@2	10.75.23.3/24	MASTER
OPT3@3	10.75.21.3/29	MASTER
OPT4@4	10.75.22.3/24	MASTER

2. Forcer l'utilisation des adresses IP virtuelles

Maintenant que les adresses IP virtuelles (VIP) sont définies, la prochaine étape cruciale consiste à configurer pfSense pour qu'il les utilise activement à la place des adresses IP propres à ses interfaces physiques.

Concrètement, cela implique de :

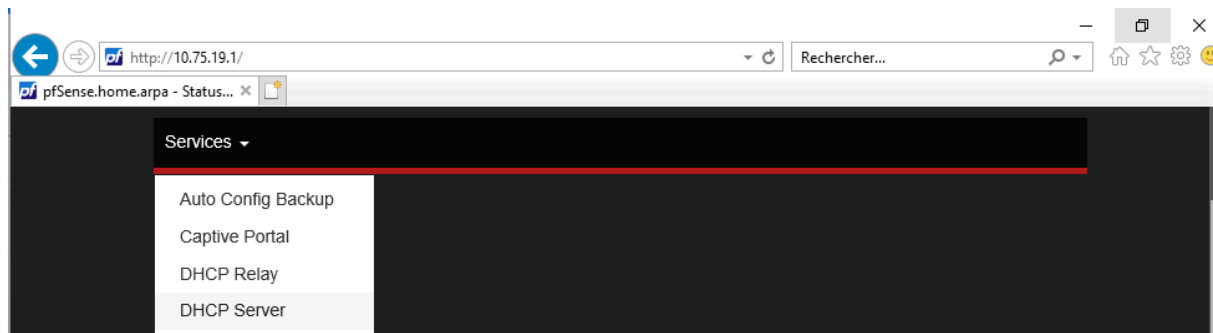
- Diriger le trafic entrant vers l'adresse VIP de l'interface LAN.
- Ajuster les différents services fonctionnant sur pfSense (comme le service DHCP) afin qu'ils utilisent l'adresse VIP de l'interface LAN comme adresse de référence.

Cette configuration garantira que, lors d'un basculement vers le serveur secondaire, les connexions établies continueront de fonctionner de manière transparente en utilisant les mêmes adresses IP virtuelles.

Configuration du service DHCP

Si pfSense gère le DHCP, il est crucial de configurer le champ "Gateway" dans "Services" > "DHCP Server" avec l'adresse VIP du LAN (10.75.23.3). Omettre cette étape maintiendrait l'ancienne adresse IP LAN pour les clients DHCP.

Optionnellement, pour synchroniser les baux DHCP, nous renseignons l'adresse IP LAN du pfSense secondaire (10.75.23.2) dans "Failover peer IP". Notons que si cette option est activée, la valeur "skew" du pfSense secondaire devra être supérieure à 20.

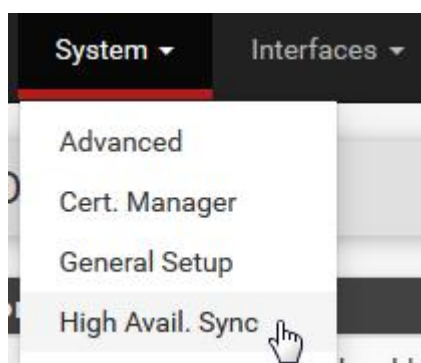


Other Options

Gateway	<input type="text" value="10.75.23.3"/>
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.	
Domain name	<input type="text" value="m2l.fr"/>
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.	
Domain search list	<input type="text"/>
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.	
Default lease time	<input type="text"/>
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.	
Maximum lease time	<input type="text"/>
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.	
Failover peer IP	<input type="text" value="10.75.23.2"/>
Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).	

3. Configurer la haute-disponibilité

Il nous reste à configurer la haute-disponibilité. Pour cela, se rendre dans "System" > "High Avail. Sync" :



Depuis cette page, il y a 2 éléments à configurer : la partie pfsync (pour la synchronisation d'état) et XMLRPC Sync (pour la synchronisation de la configuration).

State Synchronization Settings (pfsync)

- **Synchronize States :** Cochoons cette case sur les deux serveurs (primaire et secondaire) pour activer pfsync.
- **Synchronize Interface :** Nous sélectionnons l'interface à utiliser pour la synchronisation. Ici, "OPT1"
- **pfsync Synchronize Peer IP :**
 - Sur le serveur pfSense primaire (10.75.19.1), nous entrons l'adresse IP de l'interface de synchronisation du serveur secondaire (10.75.19.2)
 - Sur le serveur pfSense secondaire (10.75.19.2), nous indiquons l'adresse IP de l'interface de synchronisation du serveur primaire (10.75.19.1).
 - Si aucun IP n'est spécifié, pfSense utilisera le multicast sur l'interface sélectionnée.

Configuration de la synchronisation de la configuration (XMLRPC Sync) :

- **Synchronize Config to IP :**
 - Sur le serveur pfSense primaire (10.75.19.1), nous entrons l'adresse IP de l'interface de synchronisation du serveur secondaire (la même adresse que celle renseignée dans "pfsync Synchronize Peer IP").
 - Laissons ce champ vide sur le serveur pfSense secondaire.
- **Remote System Username :** Sur le serveur pfSense primaire (10.75.19.1), nous indiquons le nom d'utilisateur pour accéder à l'interface web du pfSense secondaire ("admin" par défaut). Laissons ce champ vide sur le serveur secondaire.
- **Remote System Password :** Sur le serveur pfSense primaire (10.75.19.1), nous entrons le mot de passe de l'utilisateur spécifié ci-dessus. Nous laissons ce champ vide sur le serveur secondaire.

Enfin, nous sélectionnons les services à synchroniser en cochant les cases correspondantes. Il est généralement recommandé de tout cocher ("Toggle All").

Exemple de résultat obtenu :

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
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.

pfsync Synchronize Peer IP
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
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
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!

Synchronize admin ☒ 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

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings

Autoriser les flux de réplication au niveau des règles du firewall

Il nous reste à autoriser les flux de répliquions sur les firewall. La configuration se passe dans "Firewall" > "Rules".

Il y a deux flux réseau à autoriser :

- le flux pour la synchronisation XML-RPC qui s'effectue via le port 443
- le flux pour la synchronisation du protocole pfsync

Sur le firewall primaire, nous créons donc une première règle de firewall (en cliquant sur le bouton "Add") avec les paramètres suivants :

- **Action :** Nous sélectionnons "Pass"
- **Interface :** Nous choisissons l'interface dédiée à la synchronisation, ici, "OPT1".
- **Address Family :** Nous laissons "IPv4"
- **Protocol :** Nous choisissons "TCP"
- **Source :** Nous indiquons l'adresse IP de l'interface de synchronisation (pour le primaire 10.75.19.2).
- **Destination :** Nous choisissons "This firewall (self)"
- **Destination port range :** Nous choisissons "HTTPS (443)" car la synchronisation XMLRPC utilise ce port.

Exemple de résultat obtenu :

Edit Firewall Rule

Action
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface
 Choose the interface from which packets must come to match this rule.

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

Protocol
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match /

Destination Port Range
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Sur le firewall primaire toujours, nous créons une seconde règle de firewall avec les paramètres suivants :

- **Action :** Nous sélectionnons "Pass"
- **Interface :** Nous choisissons l'interface dédiée à la synchronisation, ici, "OPT1".
- **Address Family :** Nous laissons "IPv4"

- **Protocol :** Nous choisissons "PFSYNC"
- **Source :** Nous indiquons l'adresse IP de l'interface de synchronisation (pour le primaire 10.75.19.2).
- **Destination :** Nous choisissons "This firewall (self)"

Exemple de résultat obtenu :

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface OPT1
 Choose the interface from which packets must come to match this rule.

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

Protocol PFSYNC
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Single host or alias 10.75.19.2 /

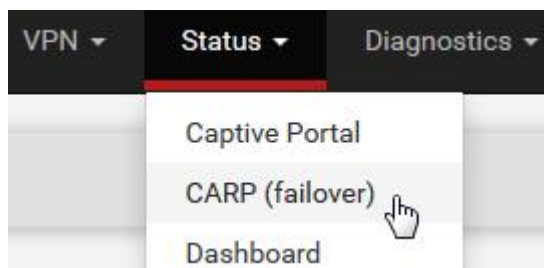
Destination

Destination ☐ Invert match This firewall (self) Destination Address /

V. Tests

Vérifier le statut du CARP (adresse VIP)

Nous pouvons vérifier l'état de nos adresses IP virtuelles depuis le menu "Status"> "CARP (failover)" :



Vérification de la réplication :

Nous accédons aux sections "Firewall" > "Rules" sur l'interface web des deux serveurs pfSense. Il faut s'assurer que toutes les règles que nous avons créées sur

le serveur pfSense primaire sont également présentes et identiques sur le serveur pfSense secondaire.

Tests de basculement :

Avant de procéder aux tests, il est fortement recommandé d'effectuer une sauvegarde de la configuration de vos deux serveurs pfSense via le menu "Diagnostics" > "Backup & Restore".

Voici quelques tests que nous pouvons effectuer pour simuler une défaillance du serveur primaire et vérifier le bon fonctionnement du basculement vers le serveur secondaire :

- **Arrêt du pfSense primaire :** Nous éteignons complètement le serveur pfSense principal. Nous vérifions que le serveur secondaire prend le relais sans interruption significative des services réseau.
- **Déconnexion des câbles réseau :** Nous débranchons le câble réseau de l'interface LAN du serveur pfSense primaire. Nous pouvons observer si le serveur secondaire assure la continuité de la connexion réseau.
- **Désactivation du service CARP :** Sur le serveur pfSense primaire, nous désactivons temporairement le service CARP via le menu "Status" > "CARP (failover)". Nous pouvons vérifier que le serveur secondaire devient actif et gère le trafic.
- **Test de continuité de service :** Pendant que nous effectuons les tests de basculement (arrêt, déconnexion, désactivation), nous lançons des actions telles que le téléchargement de fichiers ou l'exécution de commandes ping vers des hôtes externes ou internes. Il faut s'assurer que ces opérations ne sont pas interrompues ou qu'elles reprennent rapidement après le basculement.

Ces tests nous permettront de valider l'efficacité de notre configuration de haute disponibilité et de nous assurer que notre réseau reste opérationnel en cas de défaillance du serveur primaire.