



# Procédure Mise en place de redondance PfSense

## Mise en place d'une redondance de routeur PfSense

Procédure Mise en place de redondance PfSense.....	1
1- Contexte .....	1
2- IP Virtuelles .....	3
3- Règles de Pare Feu.....	5
4- Master / Backup.....	7
5- Tests .....	8
6- Conclusion.....	9

### 1-Contexte

Dans ce projet, nous allons mettre en place de la redondance pour notre routeur PfSense, afin d'assurer une haute disponibilité, via le principe d'IP virtuelle. Cela assure notamment la continuité des service lorsqu'un routeur cesse de fonctionner. La mise en place de la haute disponibilité concernant un routeur comme ici, qui est central à l'infrastructure, est très fortement recommandée.

Pour ceci, nous avons besoin de deux PfSense configurés correctement. Nous pourrons ensuite en configurer un principal (maître) et un secondaire qui prendra le relai en cas de panne (slave). Mais aussi d'un clients quelconque (ici une machine virtuelle sous Debian), afin d'accéder aux interfaces web de nos deux PfSense.

Voici la configuration de chaque PfSense que je vais utiliser :



**-PfSense A (Maître) :**

```
UMware Virtual Machine - Netgate Device ID: 69a368158a65c8fac53e
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.101.133.141/21
LANCLT (lan)   -> em2      -> v4: 192.168.10.254/24
LANSRV (opt1) -> em3      -> v4: 192.168.100.254/24
```

**Interfaces:**

EM0 => **Network:** Bridge-Wifi / **MAC:** 00:0C:29:06:65:CD / **IP :** DHCP

EM1 => **Network :** LAN-CLT / **MAC:** 00:0C:29:06:65:E1 / **IP :** 192.168.10.254

EM2 => **Network :** LAN-SRV / **MAC:** 00:0C:29:06:65:EB / **IP :** 192.168.100.254

**-PfSense B (Slave):**

```
UMware Virtual Machine - Netgate Device ID: fc9884efe2da0604f476
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.101.135.32/21
LANCLT (lan)   -> em2      -> v4: 192.168.10.252/24
LANSRV (opt1) -> em3      -> v4: 192.168.100.252/24
```

**Interfaces:**

EM0 => **Network:** Bridge-Wifi / **MAC:** 00:0C:29:7C:AD:74 / **IP :** DHCP

EM1 => **Network :** LAN-CLT / **MAC:** 00:0C:29:7C:AD:88 / **IP :** 192.168.10.252

EM2 => **Network :** LAN-SRV / **MAC:** 00:0C:29:7C:AD:92 / **IP :** 192.168.100.252

Nous allons nous assurer que le client sort sur le Web, en configurant un client par PfSense.

**-Client 1 (configuré sur le PfSense A) :**

Adresses			
Adresse	Masque de réseau	Passerelle	
192.168.10.1	255.255.255.0	192.168.10.254	⊗

Le client est correctement configuré, ping bien l'interface du PfSense, et sort sur le Web.



## 2-IP Virtuelles

Durant cette étape, nous allons créer les deux IPs virtuelles qui nous serviront pour la synchronisation entre nos deux PfSense via les LAN. Elles remplaceront aussi nos passerelles actuelles sur les clients que nous avons configurés.

### -Sur le PfSense A (maître) :

Firewall / Virtual IPs / Edit

#### Edit Virtual IP

Type  IP Alias  CARP  Proxy ARP  Other

Interface: LANCLT

Address type: Single address

Address(es): 192.168.10.253 / 24  
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password: [password] Confirm [password]  
Enter the VHID group password.

VHID Group: 1  
Enter the VHID group that the machines will share.

Advertising frequency: Base: 1 Skew: 0  
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: LAN-CLT  
A description may be entered here for administrative reference (not parsed).

Save

Firewall / Virtual IPs / Edit

#### Edit Virtual IP

Type  IP Alias  CARP  Proxy ARP  Other

Interface: LANSRV

Address type: Single address

Address(es): 192.168.100.253 / 24  
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password: [password] Confirm [password]  
Enter the VHID group password.

VHID Group: 2  
Enter the VHID group that the machines will share.

Advertising frequency: Base: 1 Skew: 0  
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: LAN-SRV  
A description may be entered here for administrative reference (not parsed).

Save

*N'oubliez pas de sauvegarder les modifications\**



Nous allons ensuite faire la même configuration sur le PfSense B (Slave), qui nous servira de routeur secondaire.

**-Sur le PfSense B (Slave) :**

Firewall / Virtual IPs / Edit ?

**Edit Virtual IP**

Type  IP Alias  CARP  Proxy ARP  Other

Interface

Address type

Address(es)  /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.

Advertising frequency

Base Skew

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 description may be entered here for administrative reference (not parsed).

Firewall / Virtual IPs / Edit ?

**Edit Virtual IP**

Type  IP Alias  CARP  Proxy ARP  Other

Interface

Address type

Address(es)  /

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password. Confirm

VHID Group

Enter the VHID group that the machines will share.

Advertising frequency

Base Skew

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 description may be entered here for administrative reference (not parsed).

*N'oubliez pas de sauvegarder les modifications\**



## 3-Règles de Pare Feu

-Nous allons devoir créer 3 règles différentes pour autoriser du trafic spécial sur notre pare feu, afin de pouvoir mettre en place la haute disponibilité.

-Règle autorisant le protocole « **PFSYNC** », afin d'assurer la synchronisation entre les deux PfSense. Et assure que la table d'état du pare-feu (qui contient les informations sur les connexions réseaux ouvertes) est répliquée sur notre pare-feu secondaire (PfSense B).

Firewall / Rules / Edit

### 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   /

**Destination**

**Destination**  Invert match   /

**Extra Options**

**Log**  Log packets that are handled by this rule   
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**    
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**



-Règle autorisant le protocole « XMLRPC », afin de répliquer la configuration du PfSense principal vers le secondaire.

Firewall / Rules / Edit

### 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** LANCLT  
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** TCP  
Choose which IP protocol this rule should match.

### Source

**Source**  Invert match LANCLT subnets Source Address /

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 This Firewall (self) Destination Address /

**Destination Port Range** HTTPS (443) From Custom To HTTPS (443) Custom  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

### Extra Options

**Log**  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** Autoriser XMLRPC  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**

### Rule Information

Tracking ID	1737987104
Created	1/27/25 14:11:44 by admin@192.168.10.1 (Local Database)
Updated	1/27/25 14:14:12 by admin@192.168.10.1 (Local Database)



-Règle autorisant le protocole « **CARP** ». Celui-ci permet à un groupe d'hôtes sur un même segment réseau, de partager une adresse IP.

Firewall / Rules / Edit

### 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   /

#### Destination

**Destination**  Invert match   /

#### Extra Options

**Log**  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**   
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**

#### Rule Information

<b>Tracking ID</b>	1738069878
<b>Created</b>	1/28/25 13:11:18 by admin@192.168.10.1 (Local Database)
<b>Updated</b>	1/28/25 13:11:18 by admin@192.168.10.1 (Local Database)

## 4-Master / Backup

Nous allons pouvoir maintenant vérifier Que nos PfSense apparaissent bien avec les rôles qu'on leur avait attribués. Nous saurons dans le même moment, si notre configuration s'est correctement répliquée sur nos PfSense.



**-PfSense A (Master) :**

The screenshot shows the PfSense A web interface for CARP status. At the top, there are buttons for 'Temporarily Disable CARP' and 'Enter Persistent CARP Maintenance Mode'. Below is a table with the following data:

Interface and VHID	Virtual IP Address	Description	Status
LANCLT@1	192.168.10.253/24	LAN-CLT	MASTER
LANSRV@2	192.168.100.253/24	LAN-SRV	MASTER

Nous voyons qu’il apparaît comme « Master ».

Nous allons donc nous assurer que notre second PfSense apparaît bien comme « Backup »

**-PfSense B (Slave) :**

The screenshot shows the PfSense B web interface for CARP status. At the top, there are buttons for 'Temporarily Disable CARP' and 'Enter Persistent CARP Maintenance Mode'. Below is a table with the following data:

Interface and VHID	Virtual IP Address	Description	Status
LANCLT@1	192.168.10.253/32	LANCLT	BACKUP
LANSRV@2	192.168.100.253/32	LANSRV	BACKUP

Il apparaît donc bien en tant que routeur de Backup. Il prendra donc le relai en cas de panne du routeur principal.

## 5-Tests

Nous allons maintenant tester nos configurations afin de vérifier si la haute disponibilité fonctionne correctement.

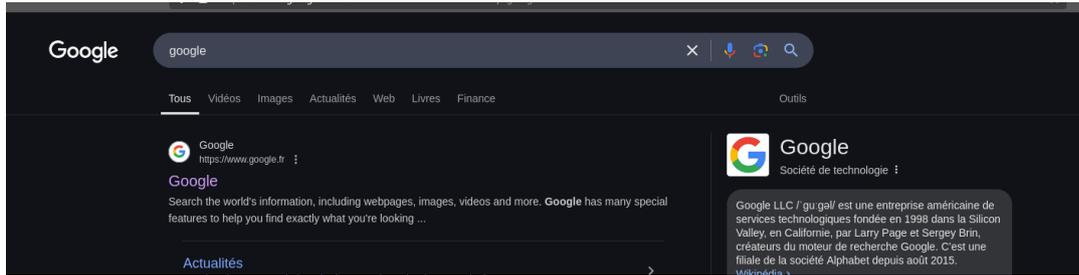
Je commence par éteindre le PfSense principal (PfSense A), afin de simuler une panne.

J’accès ensuite à l’interface web du second (PfSense B). Nous pouvons donc voir qu’il est passé en tant que « Master » :

The screenshot shows the PfSense B web interface for CARP status. At the top, there are buttons for 'Temporarily Disable CARP' and 'Enter Persistent CARP Maintenance Mode'. Below is a table with the following data:

Interface and VHID	Virtual IP Address	Description	Status
LANCLT@1	192.168.10.253/32	LANCLT	MASTER
LANSRV@2	192.168.100.253/32	LANSRV	MASTER

J’essaye ensuite de sortir sur le web via mon client pendant que le PfSense principal est éteint.



Mon client sort bien sur le web.

Le PfSense secondaire prend donc bien le relai, pour assurer le routage.

## 6-Conclusion

Nous avons donc mis en place la haute disponibilité sur notre routeur PfSense, en configurant un principal (PfSense A) et un secondaire (PfSense B). Nous nous sommes ensuite assuré que le routeur secondaire prenait bien le relai lorsque le principal était éteint. Après avoir fait ces tests, tout semble fonctionner correctement.

Nous avons donc ajouté une sécurité supplémentaire sur un matériel central de l'infrastructure réseau.