



Ayoub Belbachir

CARP pfsync

Cours : **BLOC 1**Professeur : **M. A. Ouldcheikh**Date : **17/02/2022**

INTRO

nous allons configurer la haute disponibilité dans pfSense à l'aide du protocole CARP (Common Address Redundancy Protocol) et du protocole pfsync.

Ce laboratoire suppose que vous avez déjà installé et configuré les paramètres de pare-feu de base tels que les attributions d'adresses IP, à la fois WAN et LAN.

Le but du Failover, c'est donc de faire en sorte que si mon pfSense-01 venait à tomber, le 02 prendrait le relais,

Pour cela, il existe le protocole **CARP**, pour *Common Address Redundancy Protocol*, littéralement *Protocole de redondance d'adresses communes*. Le titre est assez clair, ce protocole permet à plusieurs hôtes d'utiliser une même IP pour effectuer de la redondance.

Ensuite, nous utiliserons les protocoles **pfSync** et **XML-RPC**, qui permettent respectivement de synchroniser l'état des connexions en cours entre deux hôtes Pfsense et pour le second de répliquer la configuration.

PRÉ-REQUIS

 Oracle VirtualBox

❖ 2 VM PFSENSE >

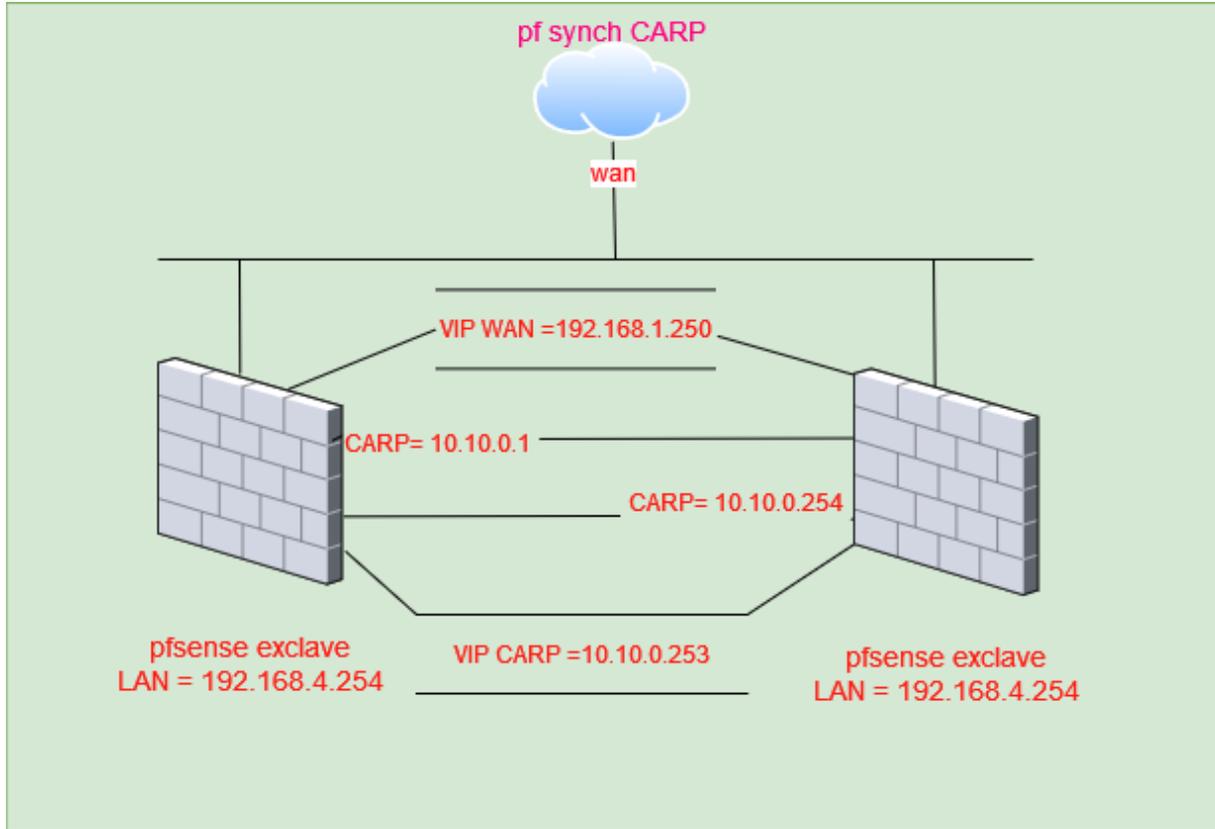
- ≥ Allocation mémoire RAM: 1go
- ≥ Stockage : 20 go
- ≥ Iso : PFSENSE
- ≥ 1^{er} Carte Réseau 'ACCÈS PAR PONT' :
- ≥ 2nd Carte Réseau « Interne » 'INET' :
- ≥ 3^{eme} Carte Réseau « Interne » 'CARP' :

❖ 1 VM windows >

- ≥ Allocation mémoire RAM : 6gb
- ≥ Stockage : 50 go
- ≥ Iso : WINDOWS 10
- ≥ 1^{er} Carte Réseau « Interne » 'INET' :

CARP pfsync

SCHÉMA-LOGIQUE



- **pfSense-Maitre :**

- IP WAN en : 192.168.1.75/24
- Une IP LAN en : 192.168.4.1/24
- Une IP pour la carte CARP en 10.10.0.1/30
- Une IP virtuelle pour la carte CARP en : 10.10.0.253/30
- Une IP virtuelle pour le WAN en : 192.168.4.250/24

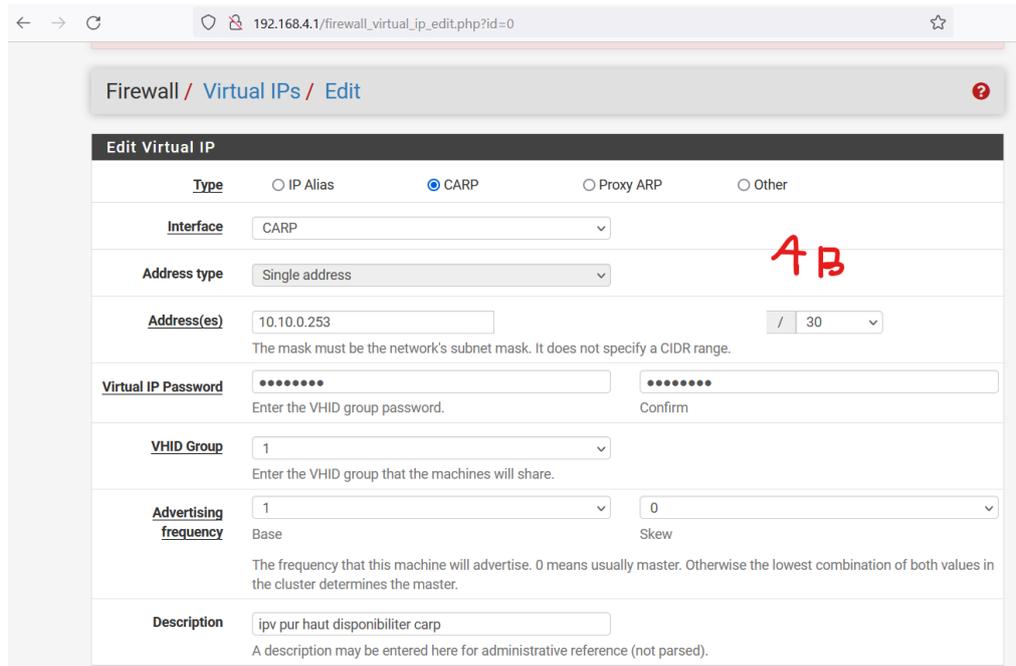
- **pfSense-Exclave :**

- Une IP WAN en : 192.168.1.76/24
- Une IP LAN en : 192.168.4.254/24
- Une IP pour la carte CARP en 10.10.0.254/30
- Une IP virtuelle pour la carte CARP en : 10.10.0.253/30
- Une IP virtuelle pour le WAN en : 192.168.4.250/24

TUTORIEL

Mise en place des interfaces virtuelles

La première étape est donc de créer nos deux interfaces virtuelles, sur chacun de nos hôtes. Pour cela on se rend sur Firewall puis Virtual IPs puis Add :



Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: IP Alias CARP Proxy ARP Other

Interface: CARP

Address type: Single address

Address(es): 10.10.0.253 / 30

Virtual IP Password: [masked] [masked]

VHID Group: 1

Advertising frequency: Base: 1 Skew: 0

Description: ipv pur haut disponibiliter carp

Ici on choisit donc le type CARP, car nous avons aussi la possibilité d'utiliser l'IP Alias ou encore le Proxy ARP, mais ce n'est pas le cas ici. On choisit ensuite notre interface, CARP pour commencer, puis on renseigne donc l'adresse IP virtuel ainsi que le masque de sous réseau. Nous renseignons un mot de passe qui sera utilisé pour le groupe VHID. On vient ensuite justement renseigner l'ID de ce fameux groupe, car un même Pfsense peut faire partie de plusieurs clusters, pour l'interface Carp nous renseignons de l'ID 1 et pour l'interface wan nous renseignons de l'ID 2. Et enfin, nous laissons la valeur Base à 1 (qui correspond au nombre de secondes avant qu'un hôte soit considéré comme down) et pour la valeur Skew, nous la laissons à valeur à 0. Cette valeur devra être modifier pour le Pfsense esclave à savoir Skew=100, ici nous sommes sur notre Pfsense-Maitre qui sera le master donc nous laissons cette valeur (0).

Ayoub Belbachir

CARP pfsync

Configuration pour l'interface WAN

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: IP Alias CARP Proxy ARP Other

Interface: WAN

Address type: Single address

Address(es): 192.168.1.250 / 24

Virtual IP Password: [masked] [masked]

VHID Group: 2

Advertising frequency: 1 (Base)

Description: ipx pour haut disponibilité WAN

Rendez-vous dans l'onglet Status puis CARP (failover) on devrait avoir ceci, après avoir réalisé les manipulations indiquées sur le PfSense :

Status / CARP

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
CARP@1	10.10.0.253/30	MASTER
WAN@2	192.168.1.250/24	MASTER

Et depuis le PfSense esclave :

Status / CARP

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
CARP@1	10.10.0.253/30	BACKUP
WAN@2	192.168.1.250/24	BACKUP

Ayoub Belbachir

CARP pfsync

Ensuite nous devons indiquer à Pfsense d'utiliser l'IP Virtuelle plutôt que d'utiliser son IP CARP/WAN classique. Pour cela, nous nous rendons dans Firewall puis NAT.

On choisit l'option Hybrid Outbound NAT plutôt qu'Automatic Outbound NAT, de cette manière nous allons pouvoir créer une règle qui sera prise en compte en cliquant sur Add juste en dessous de Mappings :

Edit Advanced Outbound NAT Entry			
Disabled	<input type="checkbox"/> Disable this rule		
Do not NAT	<input type="checkbox"/> 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 AP 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+IPv6 Select the Internet Protocol version this rule applies to.		
Protocol	any Choose which protocol this rule should match. In most cases "any" is specified.		
Source	Network	192.168.2.0 / 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
	<input type="checkbox"/> Not Invert the sense of the destination match.		
Translation			
Address	10.10.0.253 (ipv pur haut disponibiliter carp) 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	<input type="text"/> <input type="checkbox"/> 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.		
Misc			
No XMLRPC Sync	<input type="checkbox"/> Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.		
Description	passser par carp ipv plutot aue wan A description may be entered here for administrative reference (not parsed).		

Ayoub Belbachir

CARP pfsync

Mise en place de la High-Availability

Depuis le Pfsense maitre Rendez-vous dans System, puis High Avail.Sync :

Renseignez l'adresse IP de l'interface CARP du Pfsense esclave

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
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

[Toggle All](#)

Nous voulons que la synchronisation se face des 2 sens.

Ayoub Belbachir

CARP pfsync

Depuis le PfSense esclave Rendez-vous dans System, puis High Avail.Sync :

Renseignez l'adresse IP de l'interface CARP du PfSense Maitre

State Synchronization Settings (pfsync)	
Synchronize states	<input 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	CARP 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	10.10.0.1 AB 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	10.10.0.1 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	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 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 checked="" 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

Ayoub Belbachir

CARP pfsync

Les règles de pare-feu

Par défaut les interfaces sur Pfsense bloquent tout le trafic. nous devons nous rendre dans l'onglet Firewall puis Rules et enfin CARP et copiés les règles suivantes sur les 2 Pfsense :

Floating WAN LAN <u>CARP</u>												
Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	✓	0/0 B	IPv4	TCP	*	*	*	443 (HTTPS)	*	none	authorisation XMLRPC	
<input type="checkbox"/>	✓	0/0 B	IPv4	CARP	*	*	*	*	*	none	auth carp	
<input type="checkbox"/>	✓	0/0 B	IPv4	PFSYNC	*	*	*	*	*	none	auth pfsync	

Ces règles permettent d'autoriser le trafic des protocoles CARP PFSYNC et XMLRPC en relation avec notre synchronisation, le Protocol XMLRPC se trouve sur dans le port HTTPS (443)

Ayoub Belbachir

CARP pfsync

Test de la haute disponibilité

C Nous allons simplement créer un nouvel utilisateur au sein de notre Pfsense maître et observer qu'il se réplique bien sur le Pfsense exclave.

Rendez-vous dans l'onglet System puis User Manager :

Crée un nouvel utilisateur

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username: Ayoub

Password: [masked]

Full name: Ayoub Belbachir

Expiration date: [blank]

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Not member of: [empty]

Member of: [empty]

Certificate: No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.

Depuis le Pfsense exclave rendez-vous dans l'onglet System puis User Manager on peut observer que l'utilisateur a bien été dupliqué :

System / User Manager / Users

Users Groups Settings Authentication Servers

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

+ Add Delete