Introduction

pfSense est une distribution open-source basée sur FreeBSD, utilisée comme pare-feu et routeur. Elle propose de nombreuses fonctionnalités avancées telles que la redondance via CARP, le basculement automatique (failover), le portail captif, la synchronisation pfsync entre pare-feux, et l'intégration de systèmes de détection d'intrusion comme Snort.

Ce document présente ces fonctionnalités en détail avec des explications sur leur paramétrage et leur fonctionnement.

1. Failover basculement automatique de routeur

Configuration du failover avec CARP dans pfSense

Pour mettre en place un **failover** entre deux pare-feux pfSense, j'ai utilisé le protocole **CARP**, qui permet de partager une **IP virtuelle** entre les deux machines. En cas de panne du pare-feu principal, le secondaire prend automatiquement le relais sans interruption de service.

Préparation :

J'ai configuré deux pfSense avec les mêmes interfaces : **WAN**, **LAN** et une interface de synchronisation appelée **SYNC**.

- Le Master avait les IP : 172.16.0.4 (LAN), 192.168.2.160 (WAN), 10.10.10.1 (SYNC)
- Le Backup : 172.16.0.5, 192.168.2.161, 10.10.10.2

⚙️ **Configuration**

Sur le **pfSense Master** :

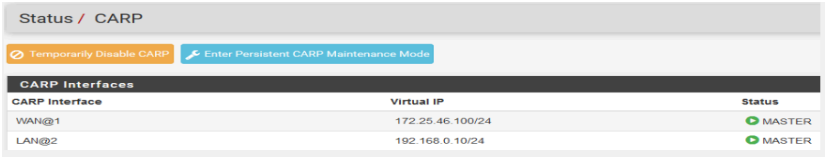
- J'ai activé la **synchronisation d'état (pfsync)** et de configuration vers le Backup via l'interface SYNC.
- J'ai ajouté les **IP virtuelles CARP** dans le menu *Firewall* > *Virtual IPs*, en choisissant le type **CARP**, un VHID unique par interface, et un mot de passe partagé.

J'ai répété la même configuration sur le **pfSense Backup**.

Résultat

Dans le menu *Status > CARP (failover)* :

- Le Master affiche **MASTER**
- Le Backup affiche **BACKUP**



J'ai testé le failover en éteignant le Master : le Backup est automatiquement passé en MASTER. Lorsque j'ai rallumé le Master, il a repris sa place principale.

Conclusion :

Cette configuration assure une **haute disponibilité** du réseau : si un pare-feu tombe, l'autre prend la relève sans coupure visible pour les utilisateurs. Grâce à **CARP et pfsync**, les IP et les connexions restent actives.

1.

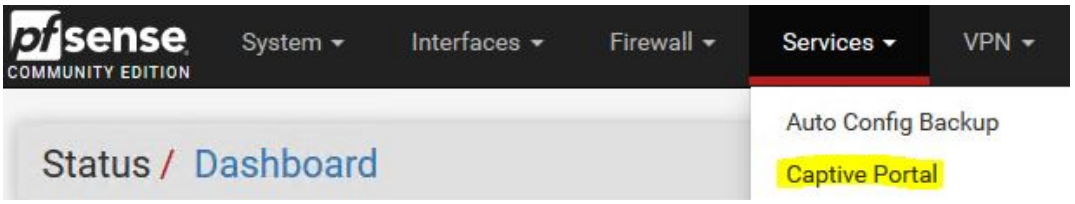
2. Portail captif

Fonction :

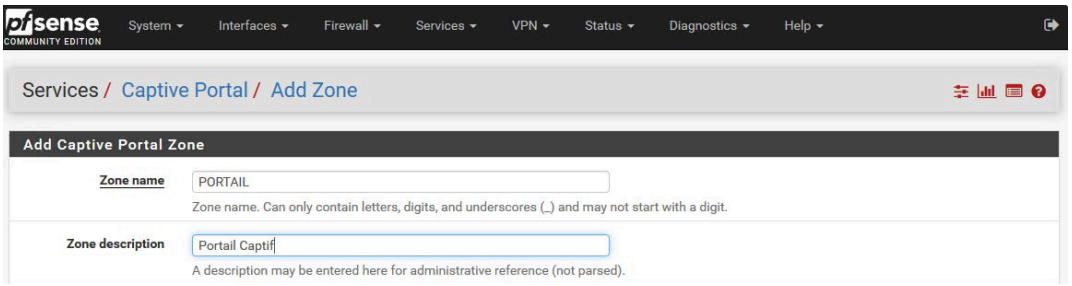
Le portail captif permet de forcer les utilisateurs à s'authentifier ou à accepter des conditions avant d'accéder à Internet.

Mise en place :

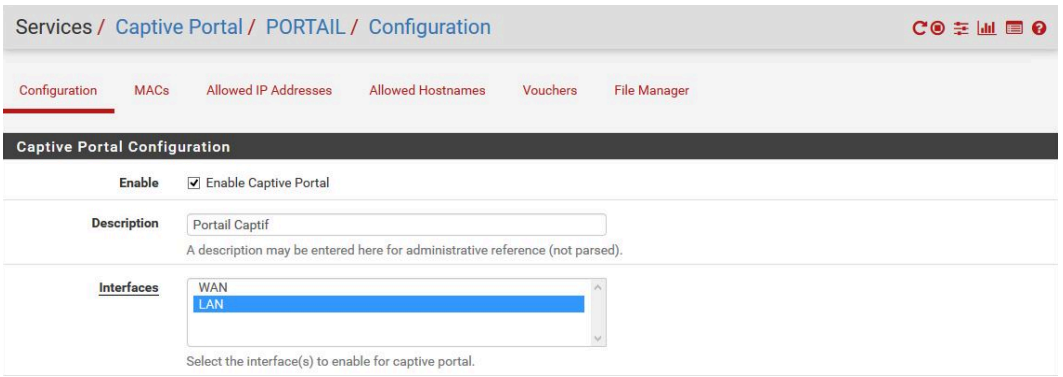
1. Aller dans Services > Captive Portal.



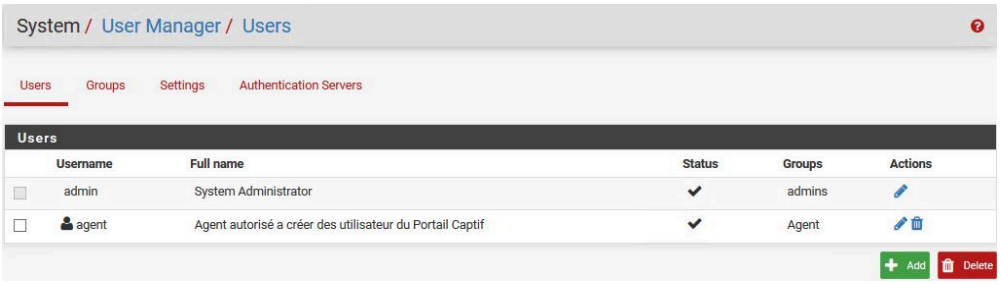
2. Créer une zone de portail.



3. Définir l'interface concernée LAN.



4. Ajouter une page d'authentification HTML ou un simple message.
5. Ajouter des méthodes d'authentification (local, RADIUS, LDAP).



6. Ajouter des exceptions si besoin (MAC, IP).
7. Prendre un client et tester si la demande d'authentification apparaît avant l'accès à internet.

3. Synchronisation avec pfsync

Fonctionnement :

pfsync permet de synchroniser en temps réel les états de connexion entre deux pare-feux. Il s'utilise souvent avec CARP pour assurer une continuité de service lors du failover.

Mise en place :

1. Créer une interface SYNC sur chaque pfSense.
2. Aller dans System > High Avail. Sync.
3. Sélectionner les options à synchroniser (règles, utilisateurs, DHCP, etc).
4. Indiquer l'adresse IP du peer sur l'interface SYNC.
5. Activer pfsync dans Interfaces > Assignments > SYNC.

4. IDS/IPS avec Snort

Fonction :

Snort permet de détecter (IDS) et prévenir (IPS) les attaques réseau en temps réel.

Installation de Snort :

1. Aller dans System > Package Manager > Available Packages.
2. Rechercher Snort et cliquer sur Install.

Configuration :

1. Aller dans Services > Snort.
2. Ajouter une interface (WAN, LAN...).
3. Activer l'interface et choisir les règles à utiliser (Snort VRT, Emerging Threats...).
4. Activer l'option Block Offenders pour passer en mode IPS.
5. Affiner les alertes et l'affichage (logging, suppression automatique...).

Conclusion

pfSense est un outil puissant pour les entreprises et les particuliers souhaitant un contrôle total sur leur infrastructure réseau. La combinaison de CARP, pfsync, portail captif et Snort permet une haute disponibilité, une sécurité avancée et une expérience utilisateur contrôlée. pfSense est une solution fiable et personnalisable.