PFSENSE

Formateur : Franck Thalmensy
Etablissement :

PFSENSE
est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD.

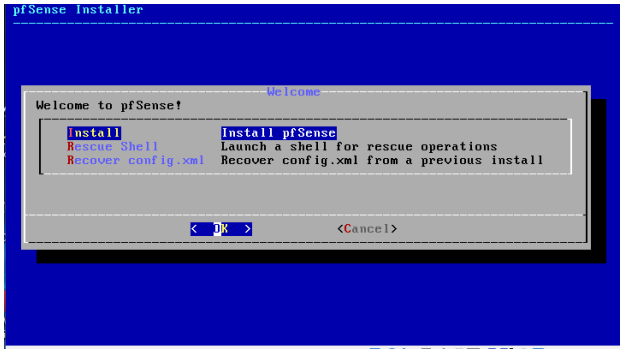
Fonctionnement :
1 site consulté = 1 connexion = 2 états (connexion entrante/sortant)
50 000 connexions = 100 000 états = ~ 100 Mo de RAM
500 000 connexions = 1 000 000 états = ~ 1 Go de RAM

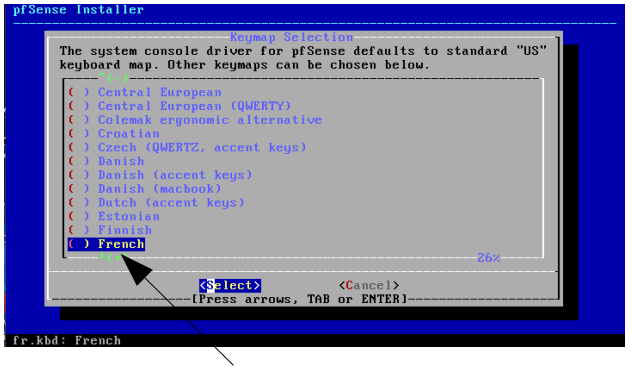
VPN :
Opter pour un processeur supportant l'AES-NI

SNORT :
Peut avoir une consommation de mémoire-vive de l'ordre de 1 à 2 Go.

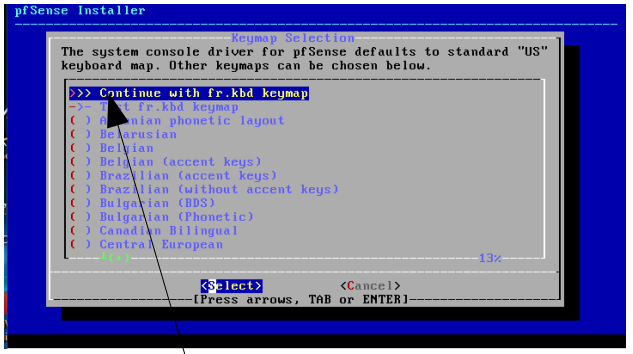
SQUID :
Squid utilise beaucoup le disque-dur (contrairement à pfSense).
il faut compter environ 15 Mo de mémoire-vive pour 1 Go de cache sur le disque-dur.

Installation

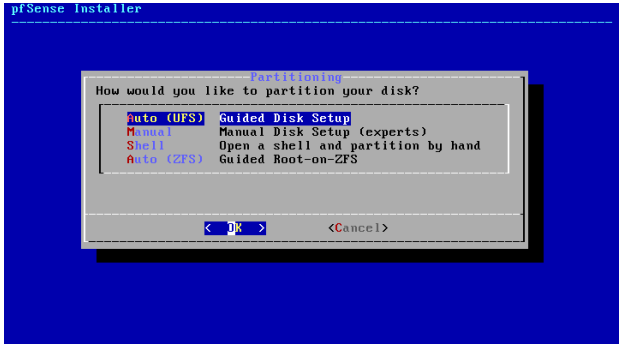


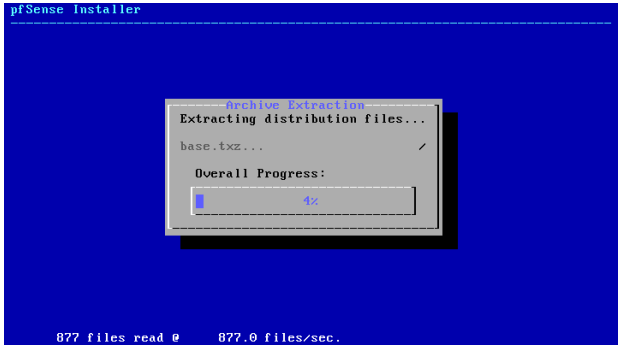


Le clavier



Continue

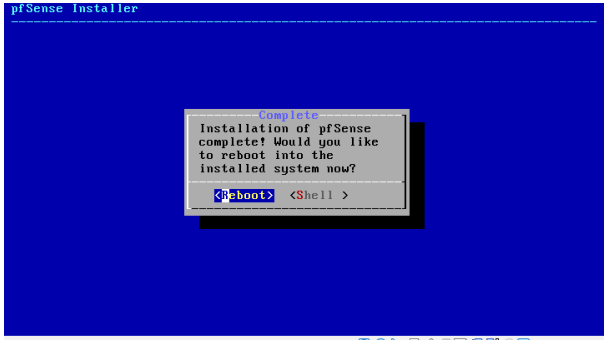




Auto (pour le formatage)

Auto (pour le formatage)

No



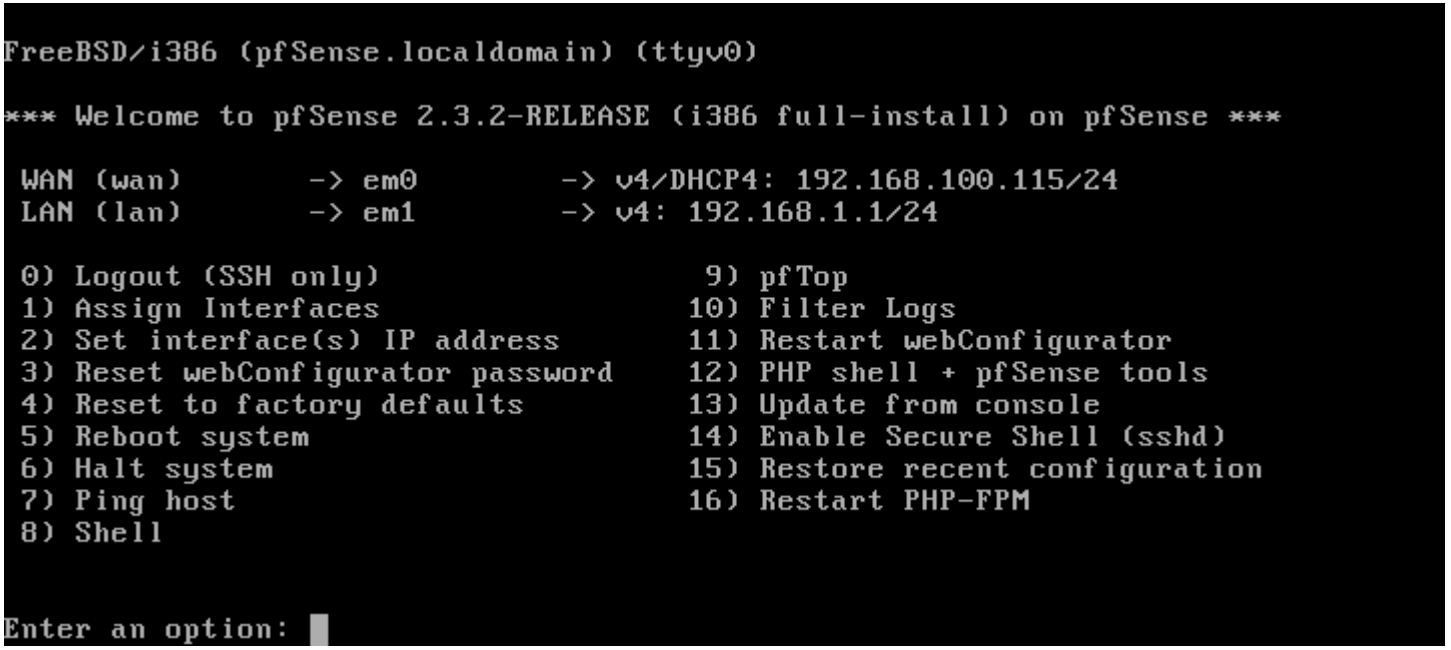
Reboot

Retirer le CD (pour ne pas repartir sur une installation)

Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN (802.1q)

(*WAN*)

(*LAN*)

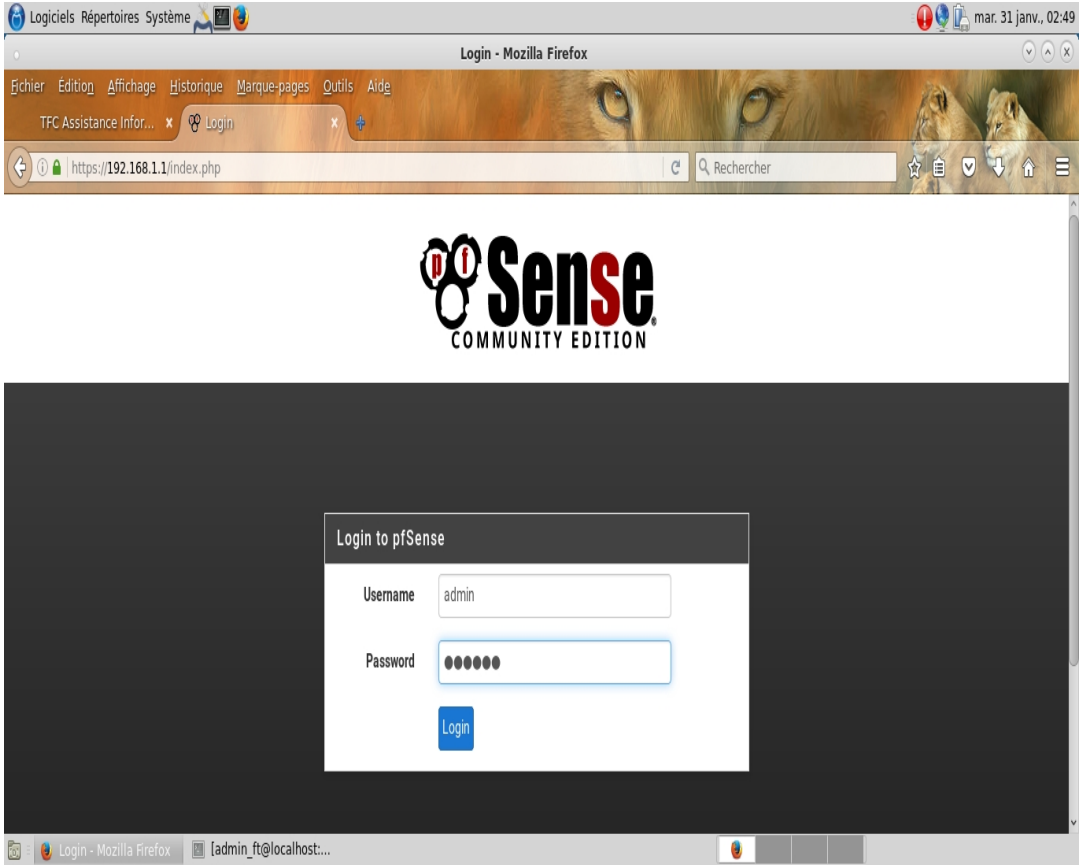


WAN correspond a l'interface réseaux connecter à internet
LAN notre réseaux

PFSENSE

L’accès web n'est possible que côté LAN

L'interface Web http://192.168.1.1



Utilisateur admin
Password pfense

Sommaire

Présentation de Pfsense

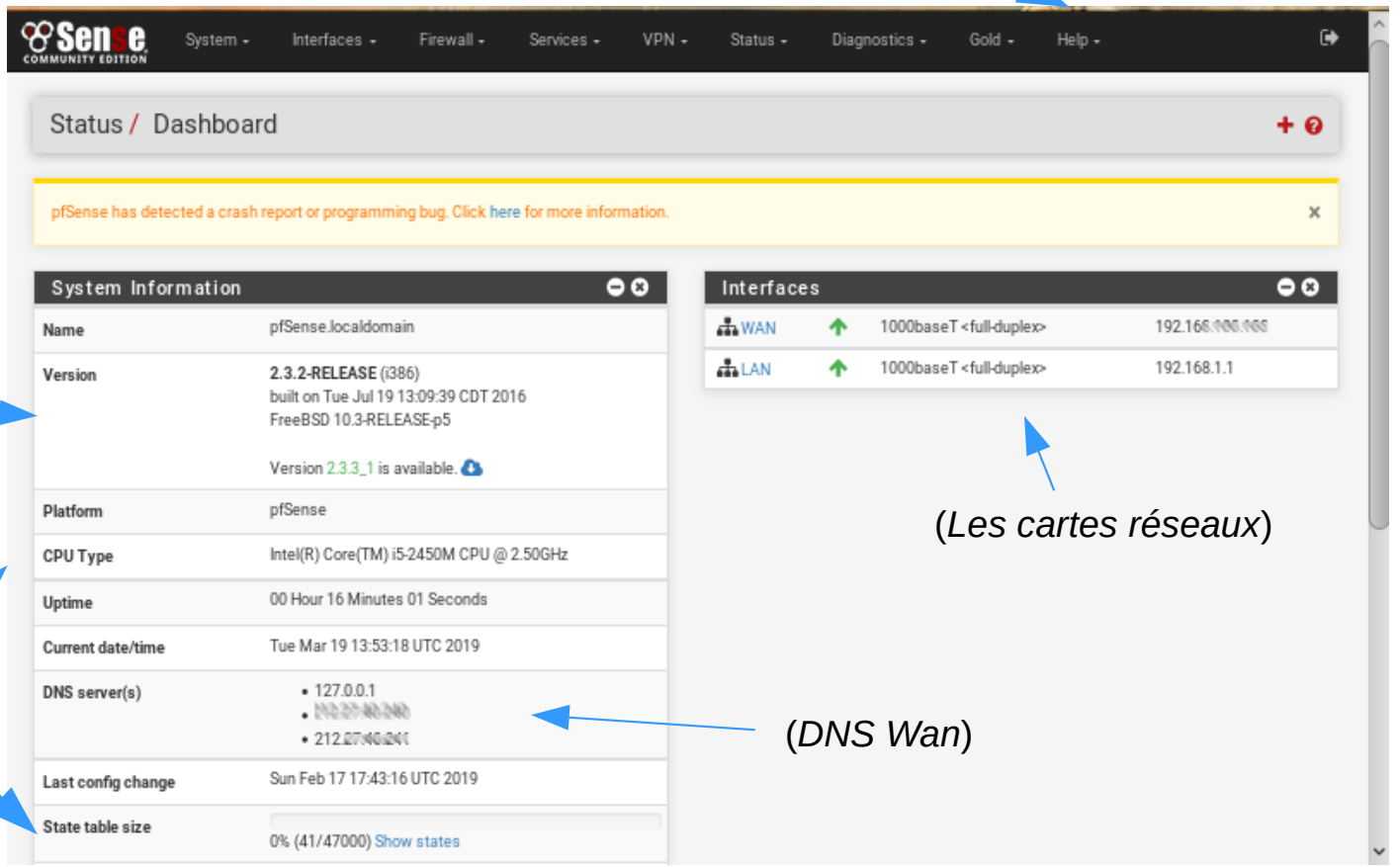
(*Les différents menus*)

(*Version de pfsense*)

(*Informations sur votre ordinateur*)

(*Les cartes réseaux*)

(*DNS Wan*)



PFSENSE

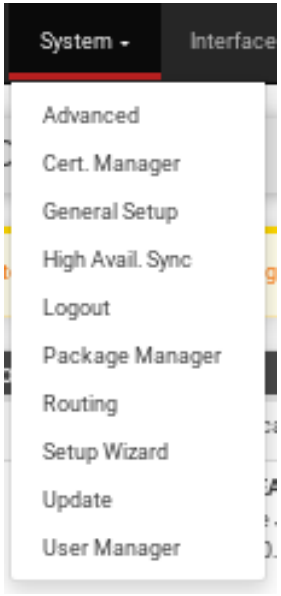
Menu

System | Interfaces | Firewall | Services

Squid

Menu

System



→ **Cert. Manager** — Permet de créer des certificats

→ **Package Manager** — Permet d'installer des paquets

Mettre le Clavier en fr

→ **User Manager** — Utilisateurs Pfsense

→ **User Manager** — Utilisateurs Pfsense

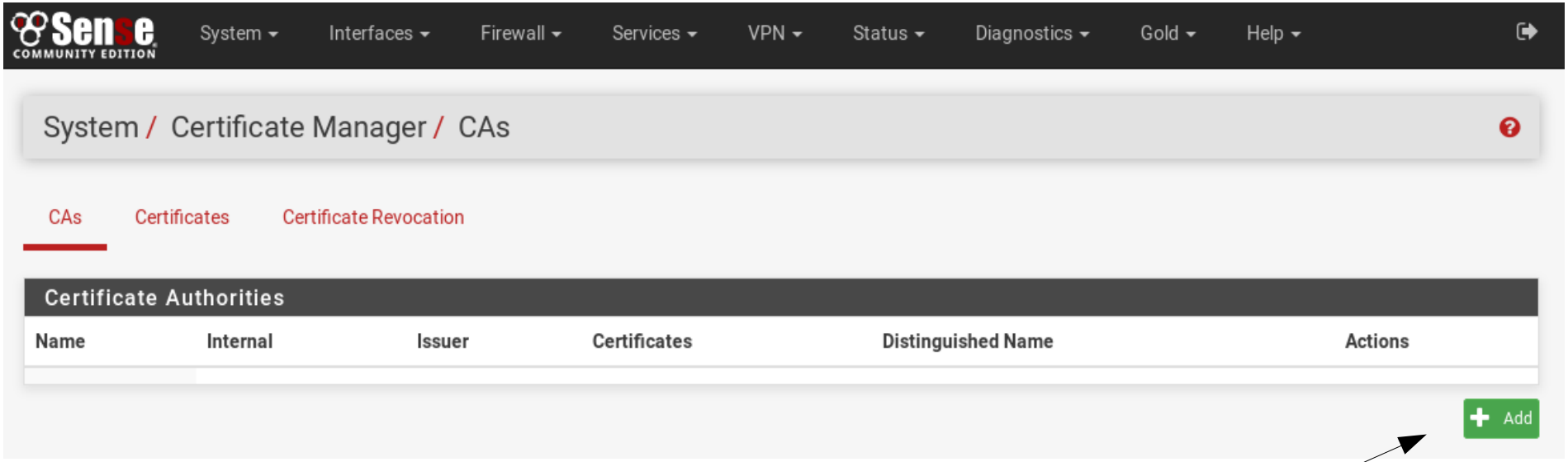
Menu

System/Cert.Manager

Création d'une autorité de certification 1/3

Les certificats SSL (Secure Sockets Layer), parfois appelés certificats numériques, sont utilisés pour créer une connexion cryptée entre le client et le serveur.

→ **CAs**

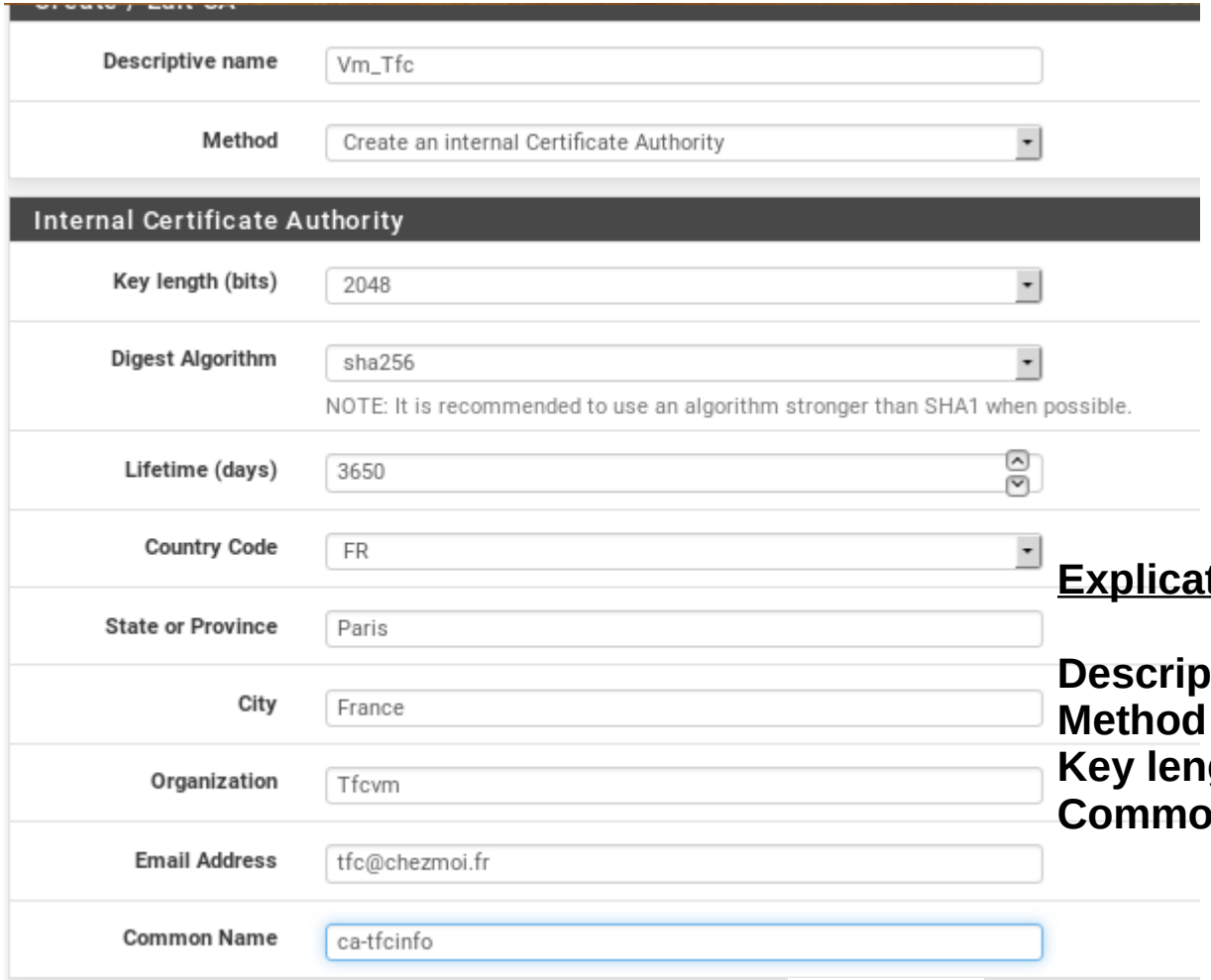


Add

Menu

System/Cert.Manager

Création d'une autorité de certification 2/3



Explication :

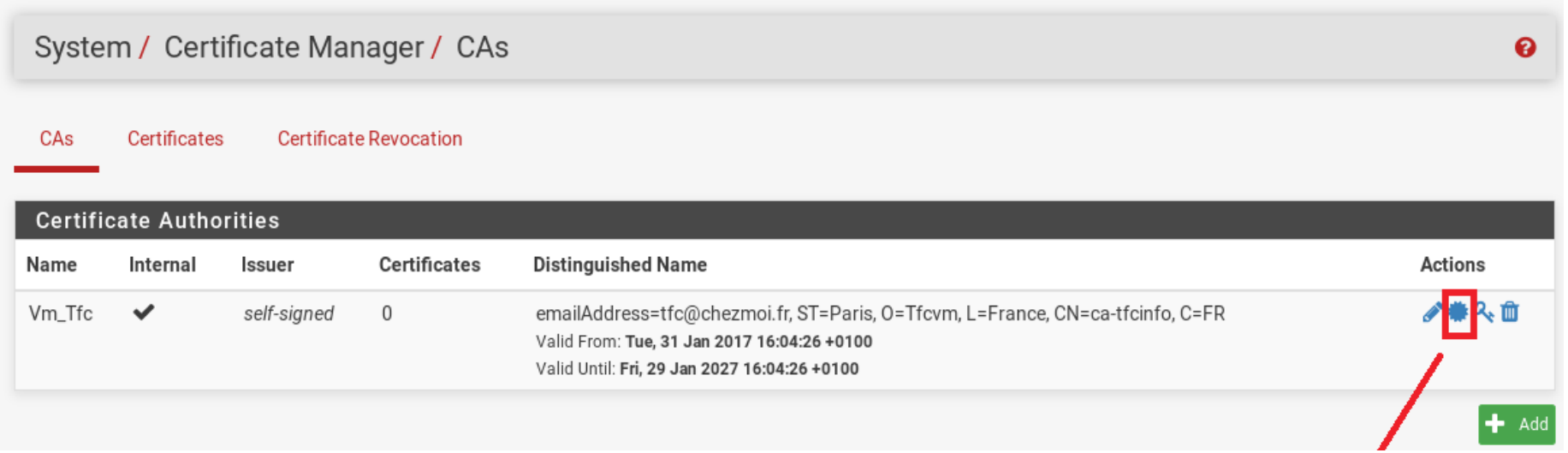
Descriptive name : Le nom (ex:Societe)
Method : Création d'un nouveaux certificat
Key lenght : Longueur de la clé de chiffrement
Common Name : sans espace et unique

Menu

System/Cert.Manager

Création d'une autorité de certification 3/3

Voici notre certificat !



Notre autorité de Certificat réussi

Après avoir fait le Cas, nous allons faire le Certificat Serveur

Menu

System/Cert.Manager

Certificat Serveur 1/4

→ **Certificates**

Add

PFSENSE

Menu

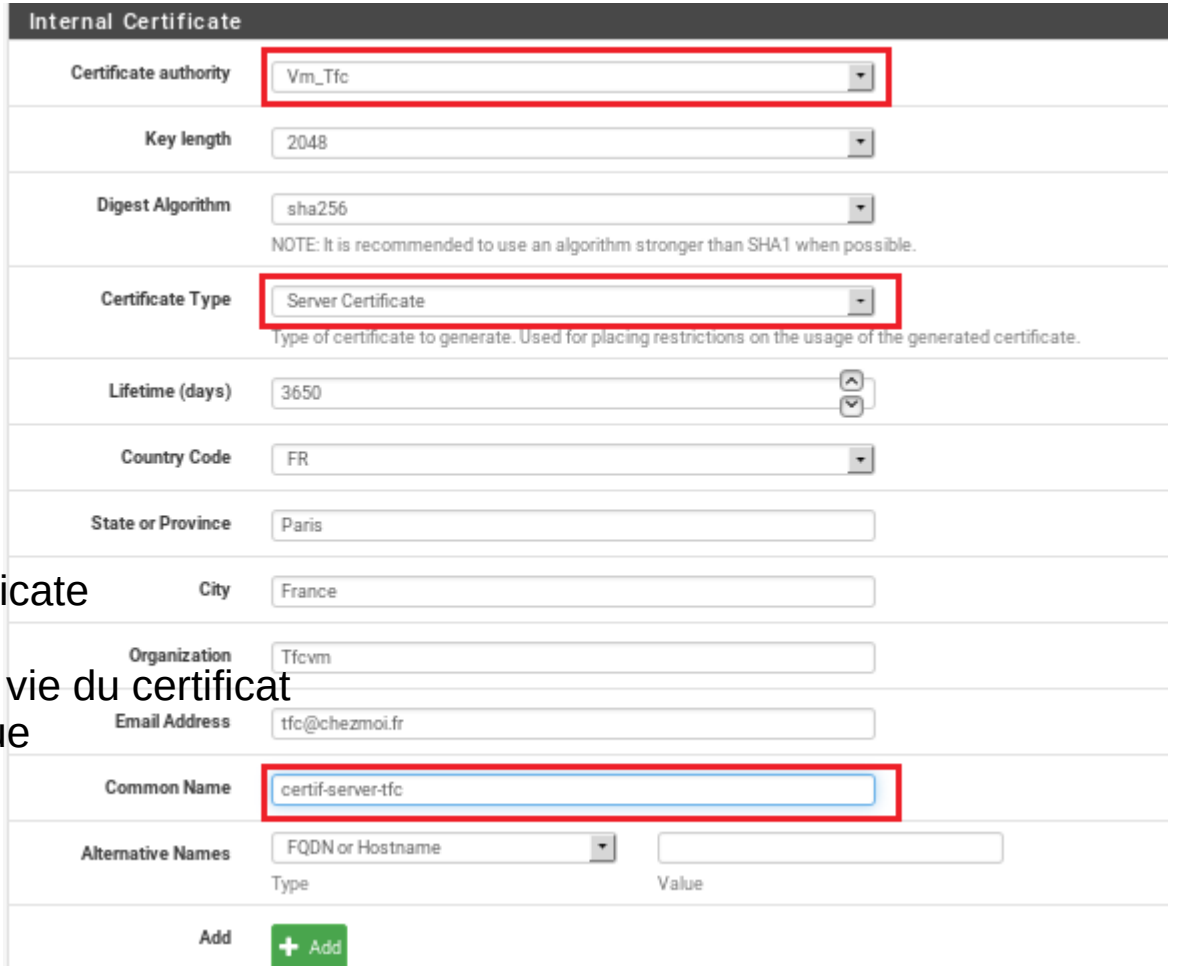
System/Cert.Manager

Certificat Serveur 2/4

Menu

System/Cert.Manager

Certificat Serveur 3/4



Explication :

Certificate authority : Notre Cas Certificate
Certificate Type : Server Certificate
Lifetime (days) : 3650 Jours, durée de vie du certificat
Common Name : sans espace et unique

PFSENSE

Menu

System/Cert.Manager

Certificat Serveur 4/4

Votre Certificat serveur est prêt

Après avoir fait le **Cas** et le **certificat** Serveur il reste le certificat client

Menu

System/Cert.Manager

Certificat Client 1/3

→ **Certificates**

System / Certificate Manager / Certificates

CAs | Certificates | Certificate Revocation

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (588fce01b1117) *Server Certificate* CA: **No**, Server: **Yes**	*self-signed*	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-588fce01b1117, C=US Valid From: **Tue, 31 Jan 2017 00:36:33 +0100** Valid Until: **Sun, 24 Jul 2022 01:36:33 +0200**	webConfigurator	
Cert (serveur) *Server Certificate* CA: **No**, Server: **Yes**	Vm_Tfc	emailAddress=tfc@chezmoi.fr, ST=Paris, O=Tfcvm, L=France, CN=certif-server-tfc, C=FR Valid From: **Tue, 31 Jan 2017 21:42:31 +0100** Valid Until: **Fri, 29 Jan 2027 21:42:31 +0100**		

Add

le certificat serveur est déjà crée

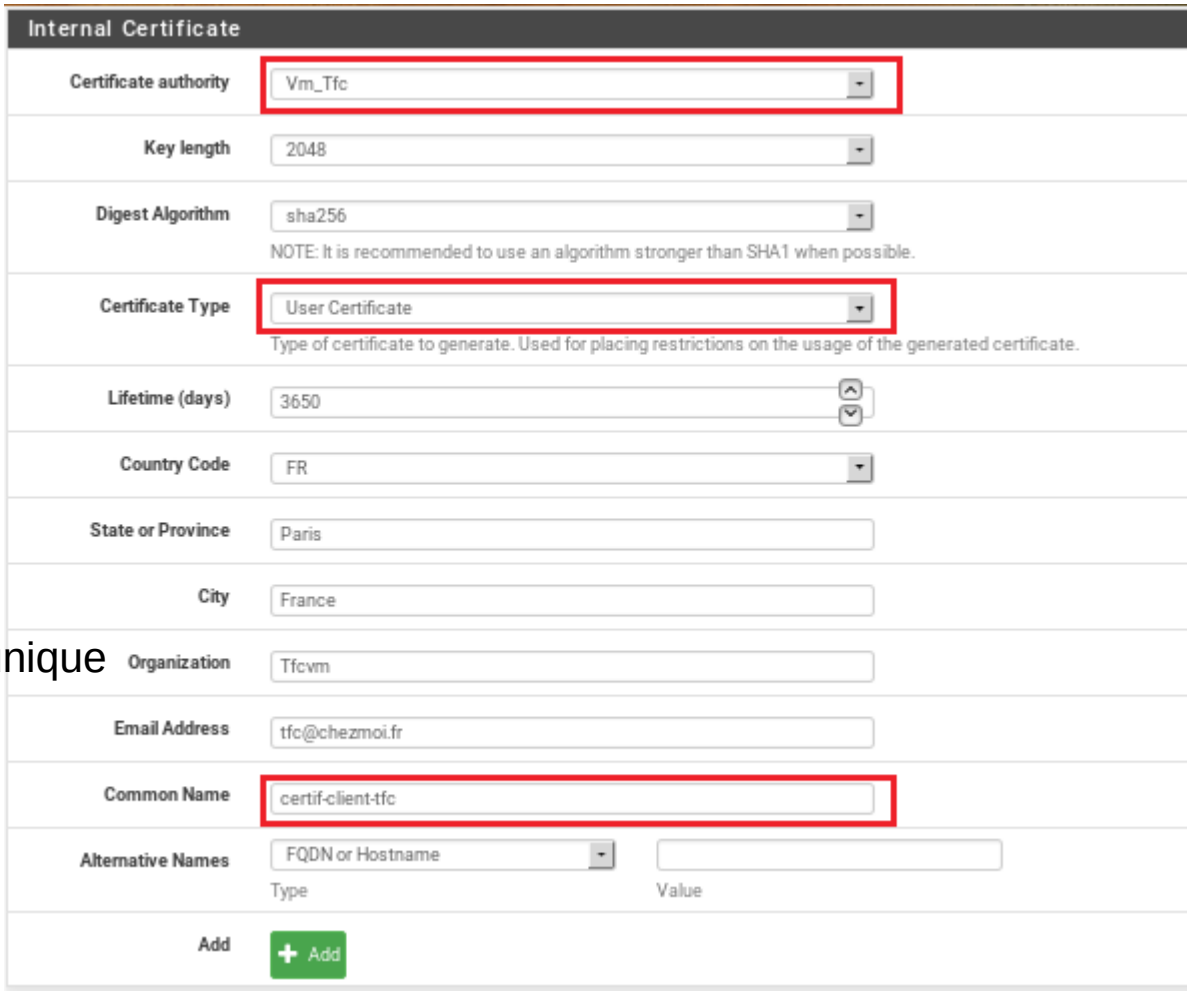
Add

PFSENSE

Menu

System/Cert.Manager

Certificat Client 2/3



Explication :

Certificate Type : User Certificate
Common Name : sans espace et unique

Add

Menu

Menu | Package Manager | Utilisateur

PFSENSE

Menu

System/Cert.Manager

Certificat Client 3/3

Votre Certificat Client est prêt

Tous les Certificats on été crée

Il ne reste plus qu'a configurer :
- Le serveur VPN
- Crée un utilisateur pour le VPN_

Menu

Menu | Package Manager | Utilisateur

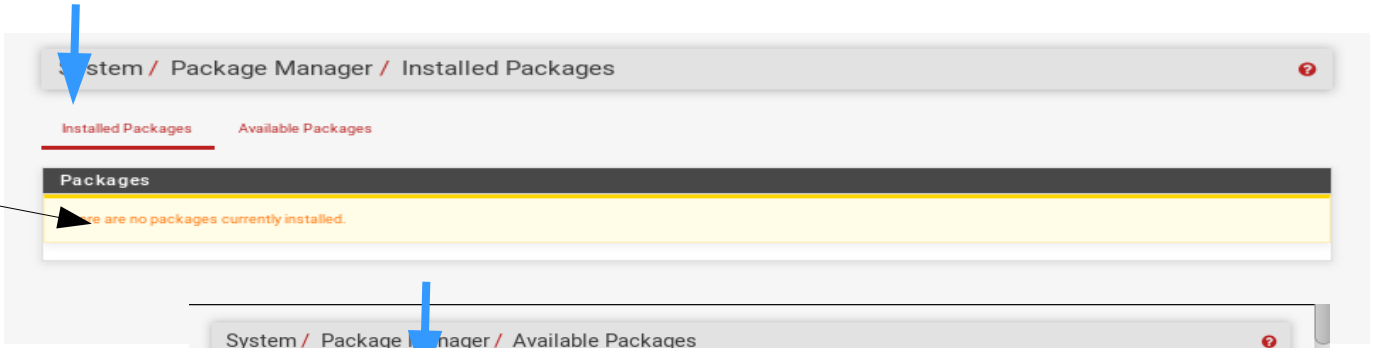
Menu

System/Package Manager

Pfsense basé sur FreeBSD donc il utilise les commande pkg pour gérer manuellement des packages FreeBSD

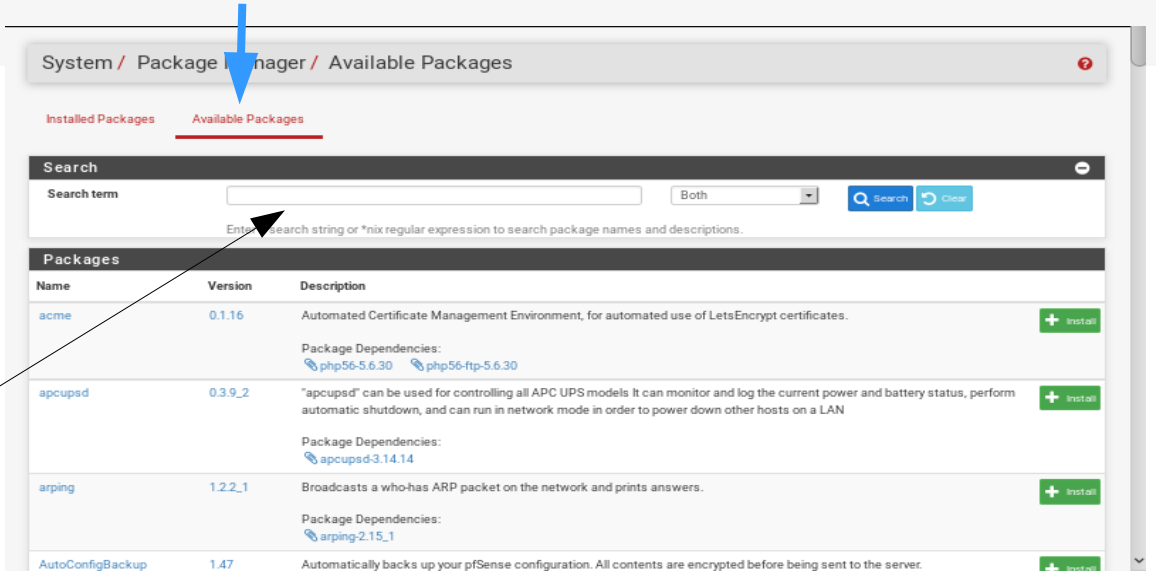
→ **Installed Packages**

(Package installer
sur votre ordinateur)



→ **Available Packages**

(Package disponible)



Vous pouvez rechercher ou parcourir la liste

Menu

System/Package Manager

Programme

Récupéré le package **squid et squidGuard**

Par deffault le Proxy (ou serveur mandataire) n'est pas installer, sur Pfsense c'est Squid
Le Proxy s'occupe :
- Du cache (désigne un espace disque dédié aux pages les plus souvent visitées)
- Du filtrage Web (se feras par les packet squid squidguard)
- Authentification
- Reverse-Proxy (Permet au utilisateur Internet d'accéder au serveur interne)

Configuration

Récupéré le package **Open-VM-Tools**

Installer Open-VM-Tools :
- Sur une machine virtuel VmWare

Configuration

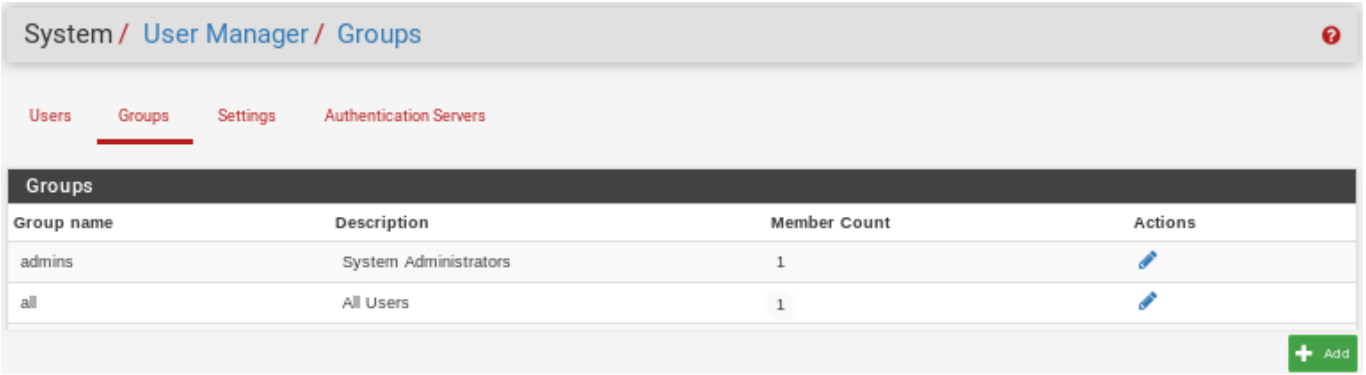
Menu

System/User Manager

Pfsense permet de gérer des utilisateurs pour vos accès Web/Vpn

(Vos utilisateurs)

(Vos Groupes)



Utilisateurs Web

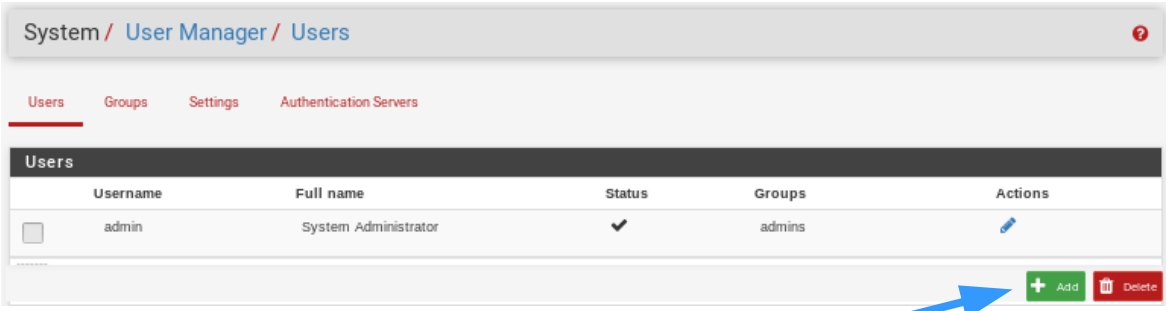
Menu | Certificat manager | Package Manager

Menu

System/User Manager

Utilisateur Captive Portal 1/5

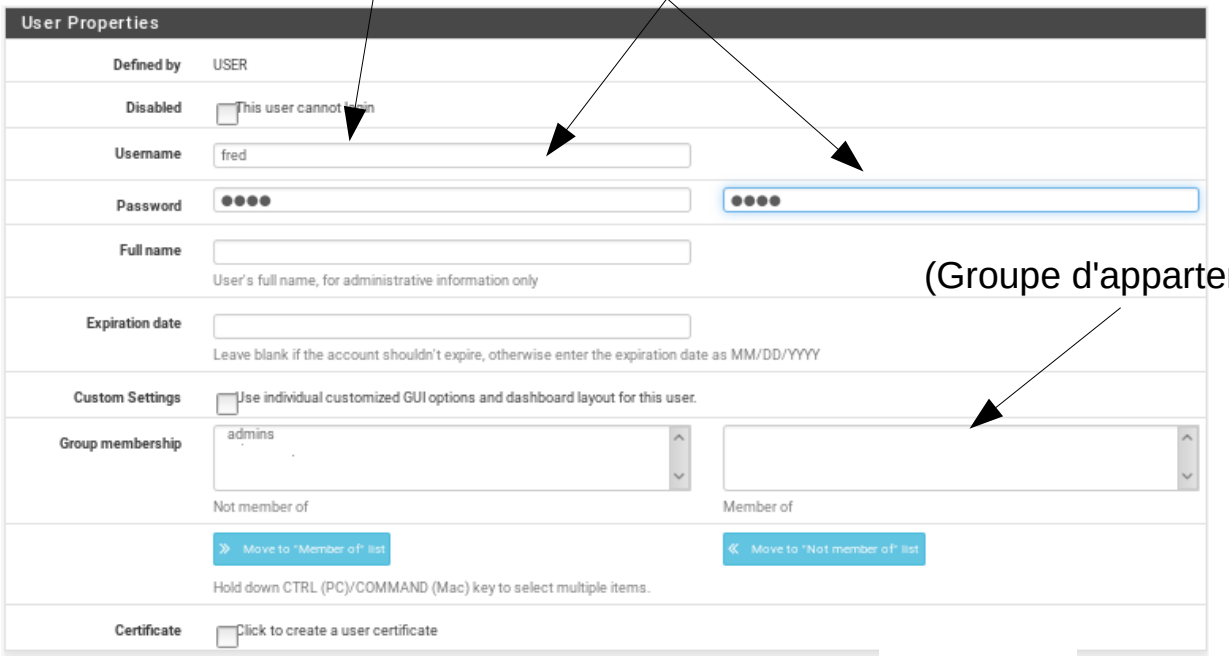
Création d'un utilisateur pour accéder à Internet (Captive Portal activé)



1) Add

(*Le nom*)

(*Password*)



(Groupe d'appartenance)

2) Save

Menu

Certificat manager

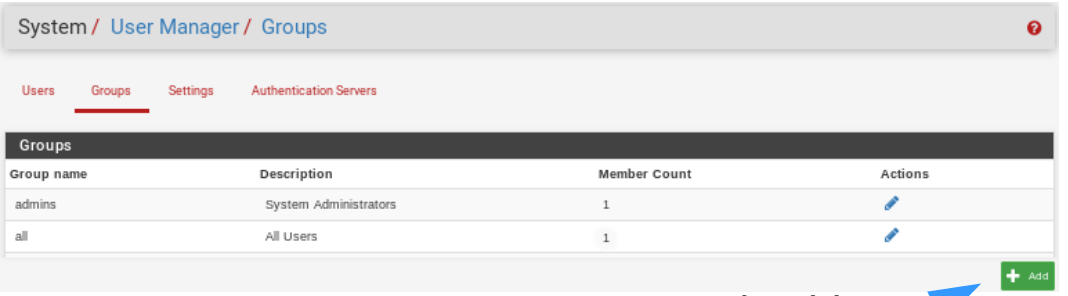
Package Manager

Menu

System/User Manager

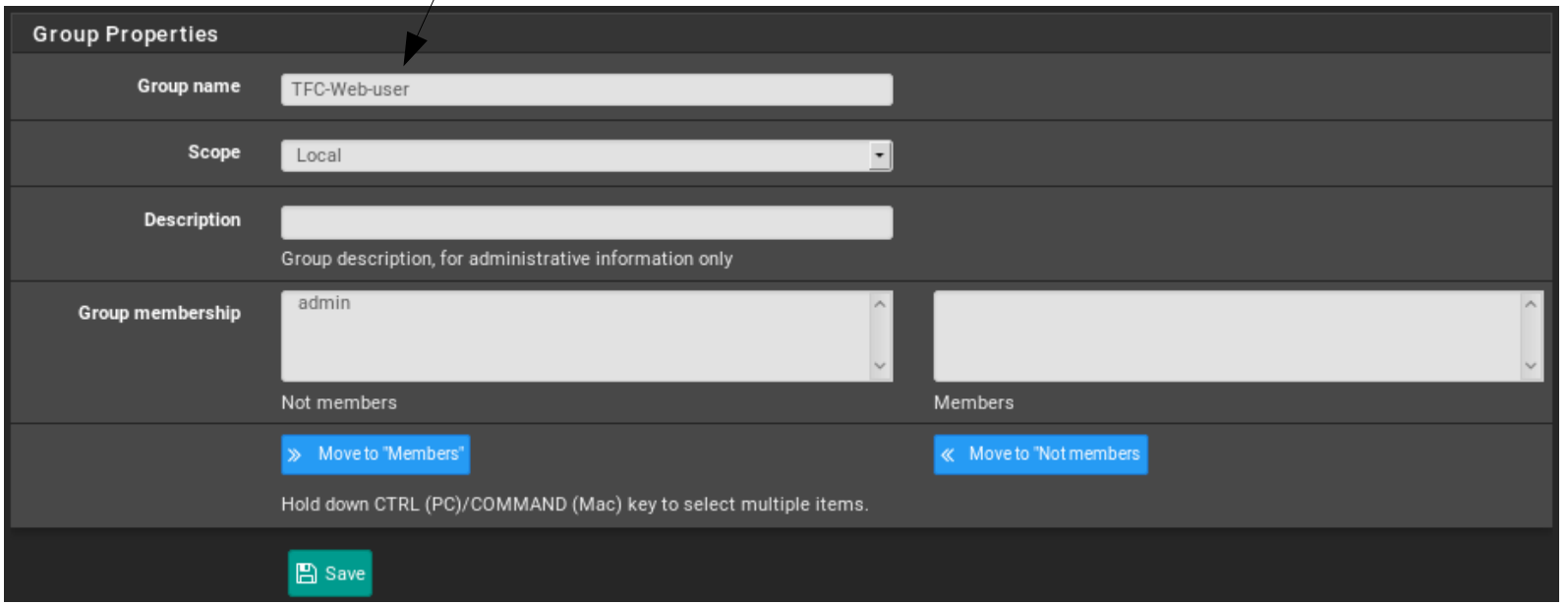
Utilisateur Captive Portal 2/5

Création du groupe (Captive Portal)



3) Add

(*Le nom du groupe*)



4) Save

Menu

Certificat manager

Package Manager

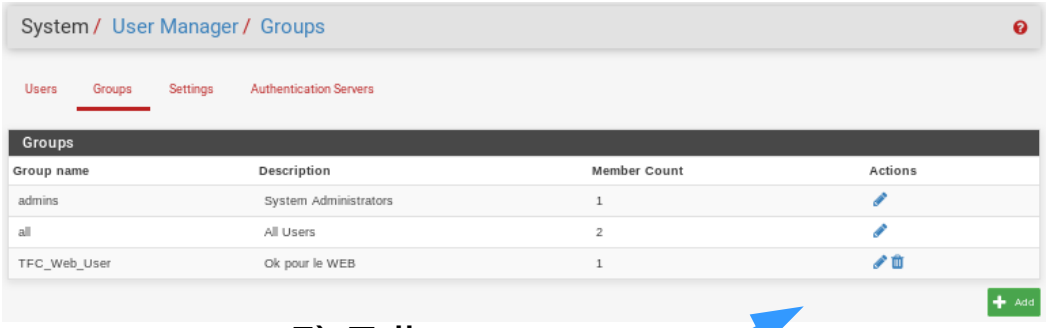
Menu

System/User Manager

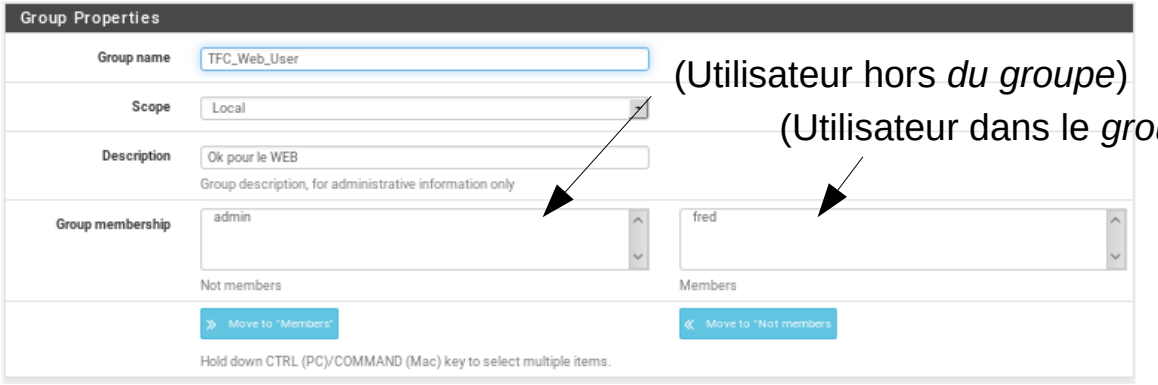
Utilisateur Captive Portal 3/5

Dès que vous avez créé le groupe nous allons ajouter

- les utilisateurs et lui attribuer la fonctionnalité Captive Portal



5) Edit group



(Utilisateur hors *du groupe*)

(Utilisateur dans le *groupe*)

6) Ajouts des utilisateurs

7) Add

Menu

Certificat manager

Package Manager

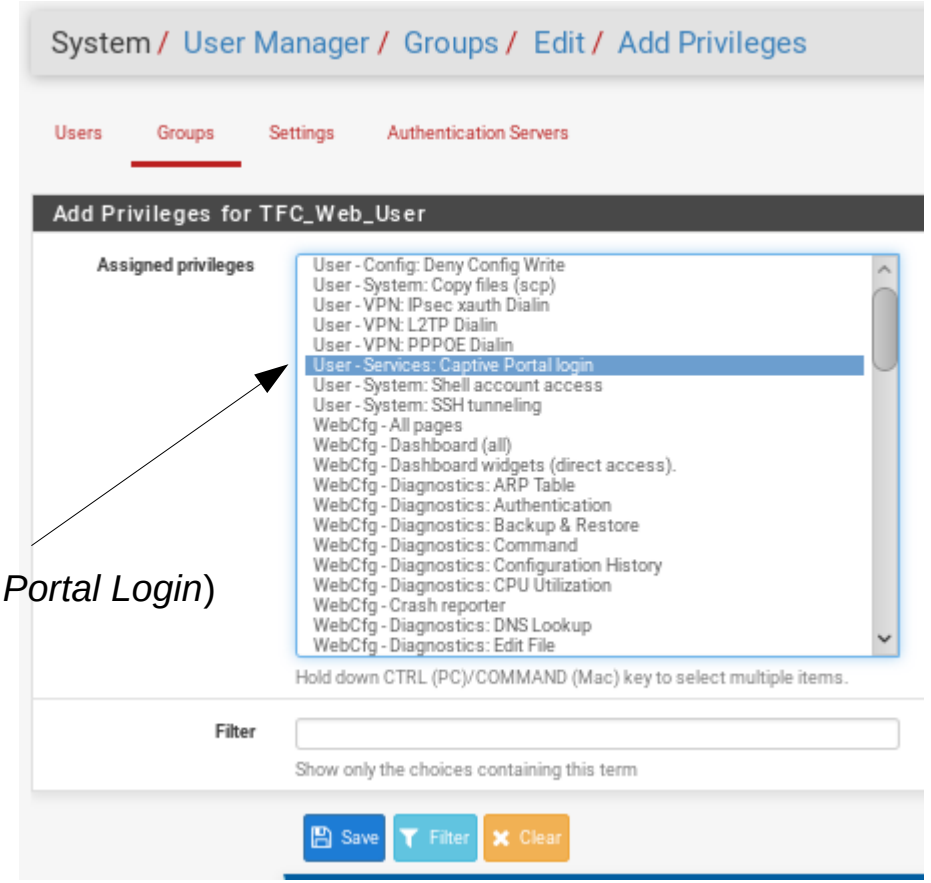
Menu

System/User Manager

Utilisateur Captive Portal 4/5

On choisie le privilège qui permet d'accéder au Portal

(*User – Services:Captive Portal Login*)

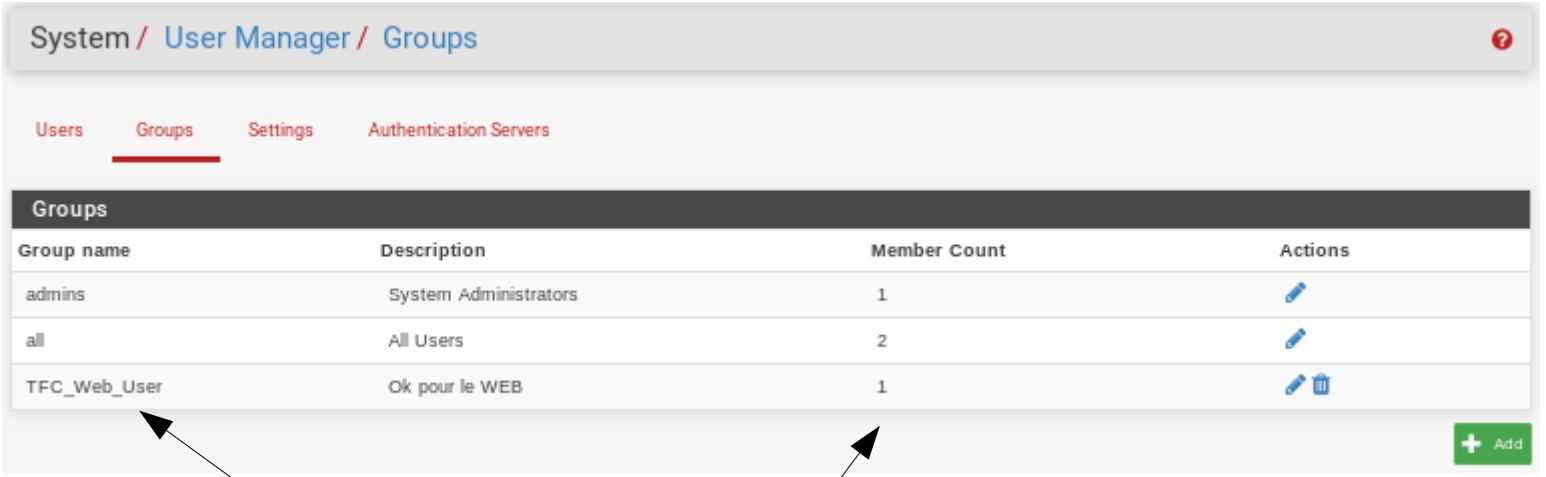


Save → 

Menu

System/User Manager

Utilisateur Captive Portal 5/5



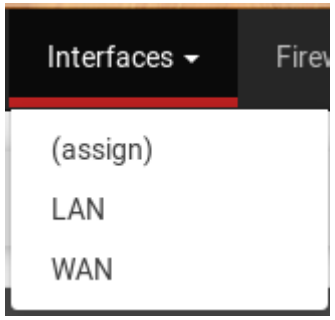
(Votre Groupes Web)

(*nbr d'utilisateurs*)

Menu

Interfaces

Permet de configurer vos différentes interface



Votre :

Wan
Lan

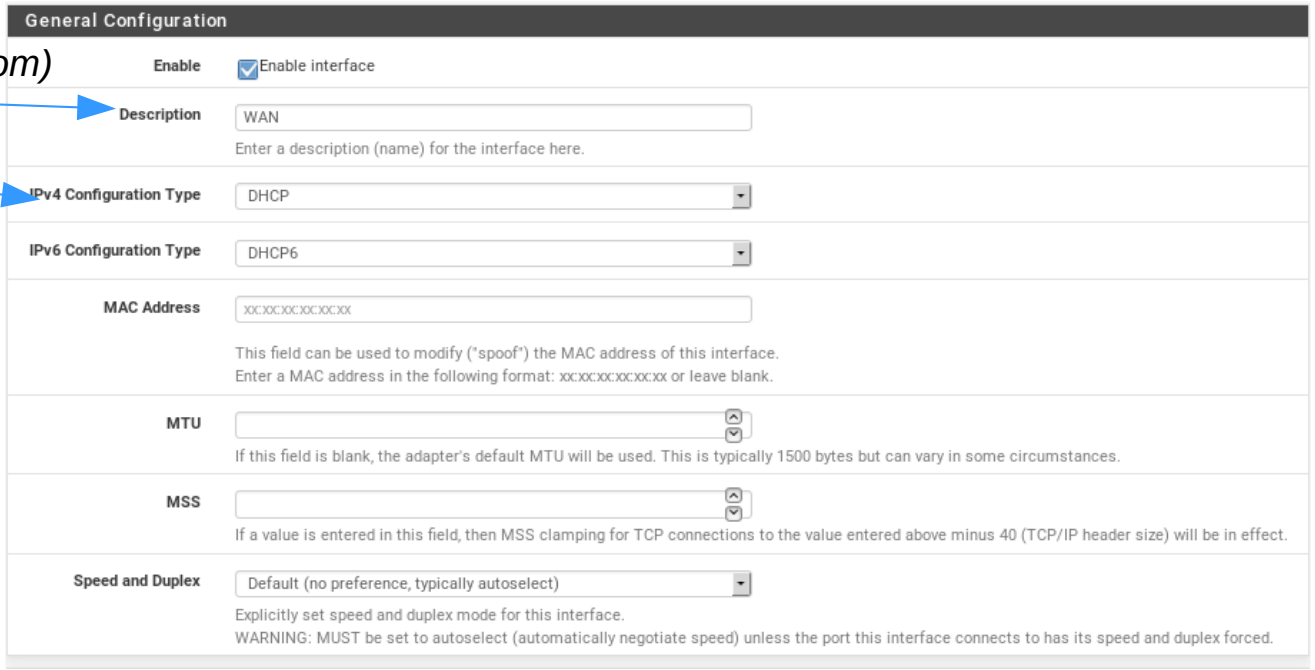
Menu

Interfaces

Les paramètres sont identique pour votre WAN/LAN

(Vous pouvez modifier le nom)

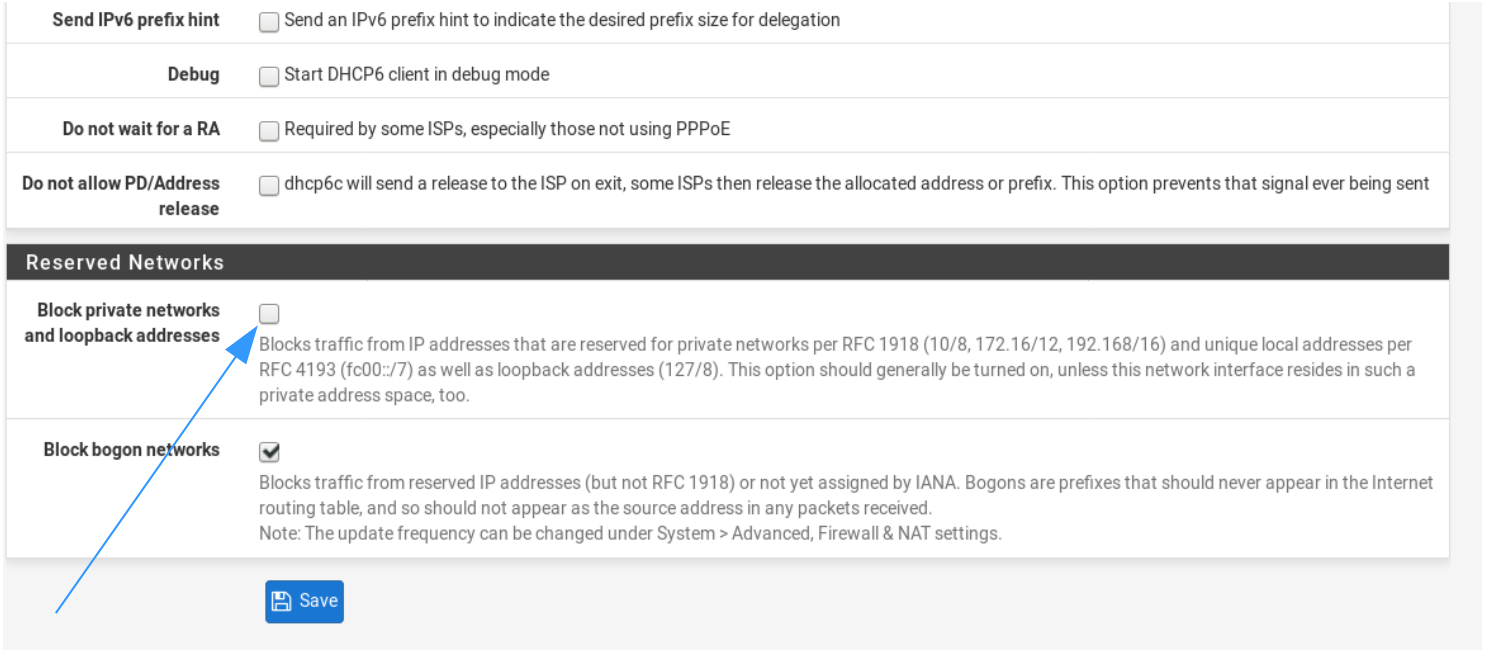
(Dhcp/Static)



Menu

Interfaces

Les paramètres sont identique pour votre WAN/LAN



décocher la case Block private networks and loopback addresses.
(pour accéder à l'interface de gestion)

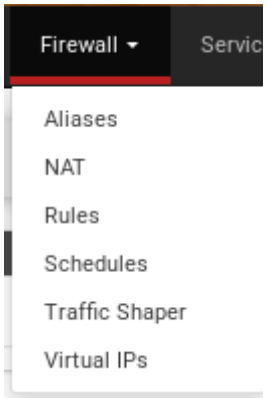
⟷ *Autorise le Port 443*

Menu

Firewall

Firewall → Rules → Lan

Permet de configurer les règles



→ **NAT** — Redirection

→ **Rules** — Règles de firewall Wan/Lan

→ **Virtual IPs** — l'équilibrage de charge (failover)

PFSENSE

Menu

Firewall/Rules

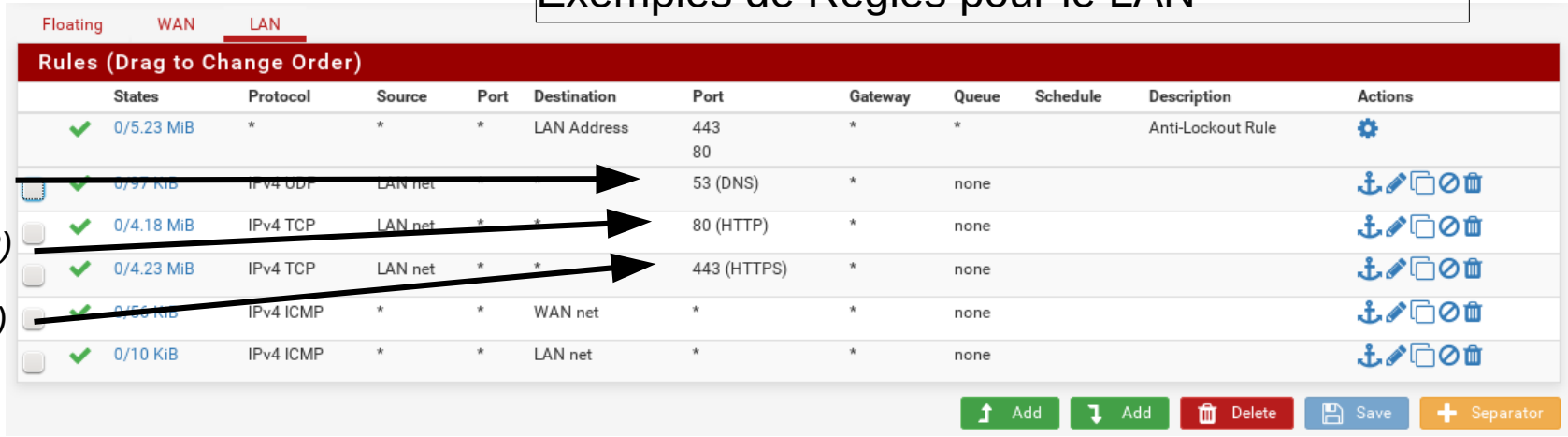
Exemples de Règles pour le LAN

(Règles sur Lan)

(Règles DNS)

(Règles HTTP)

(Règles HTTPS)



Exemples de Règles pour le WAN

(Règles sur Wan)

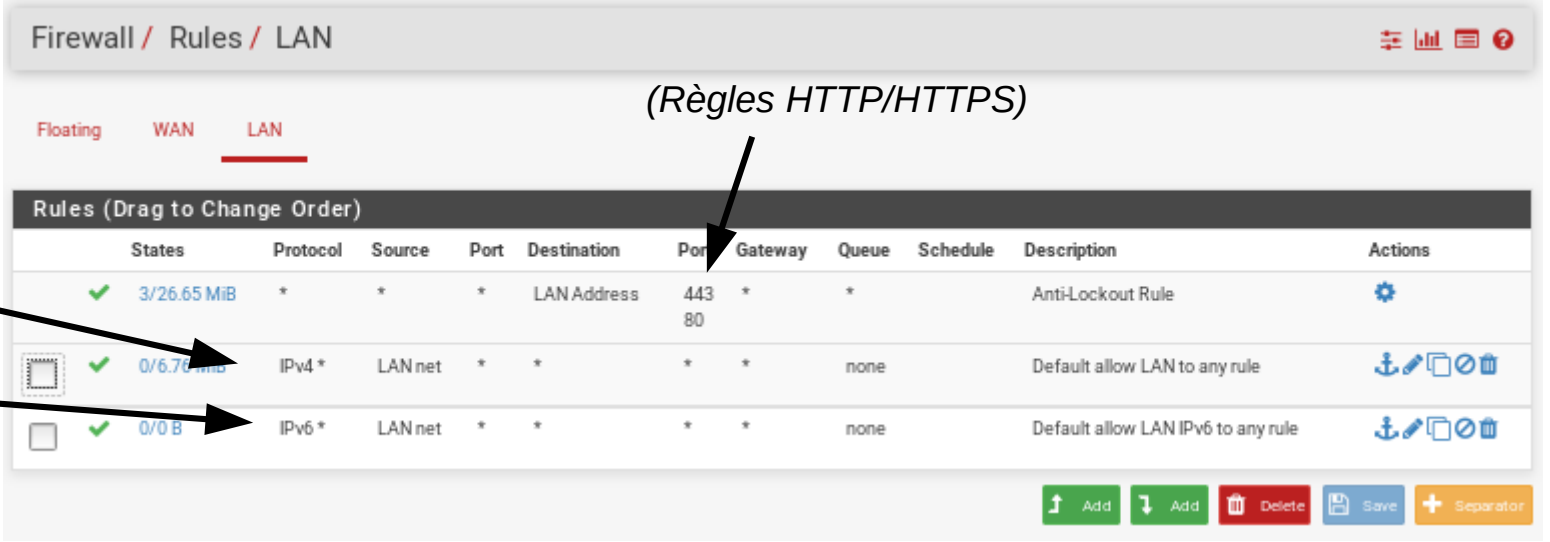
(Règles ICMP)

(Règles Nat)

Menu

Firewall/Rules/LAN

Règles par défaut pour le LAN



Les autorisation les plus haut (valide) si plus bas l'autorisation contredit la 1er elle ne seras pas prit en compte

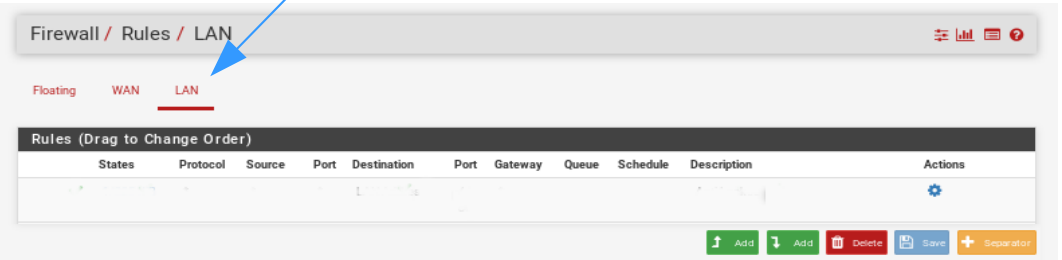
Règles HTTP/HTTPS : pour accéder à l'interface de gestion
IPv4 : tout autoriser
IPv6 : tout autoriser

PFSENSE

Menu

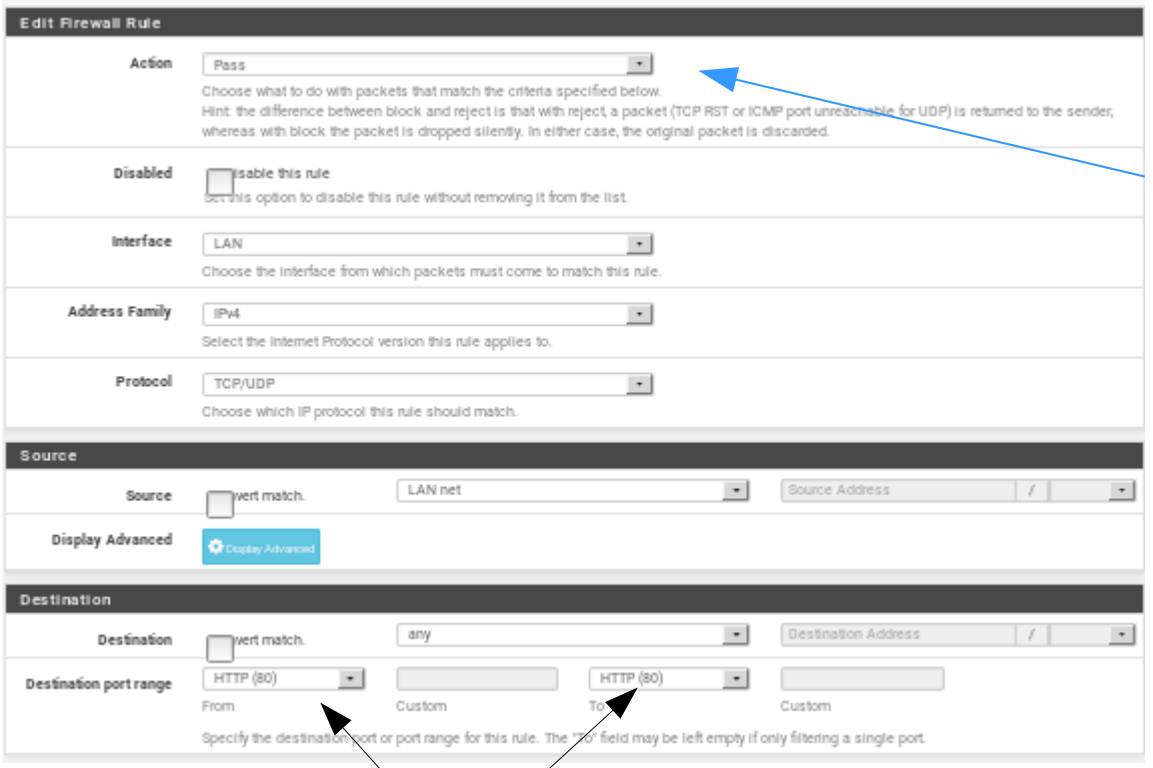
Firewall/Rules/LAN

1) Lan



2) Add

Autorisée le Port 80 sur le Lan



(Action)

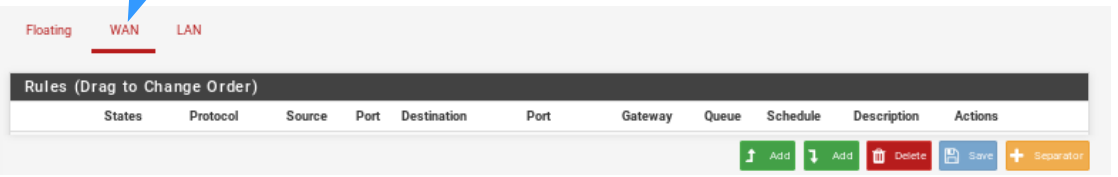
Port 80

Menu

Menu

Firewall/Rules/WAN

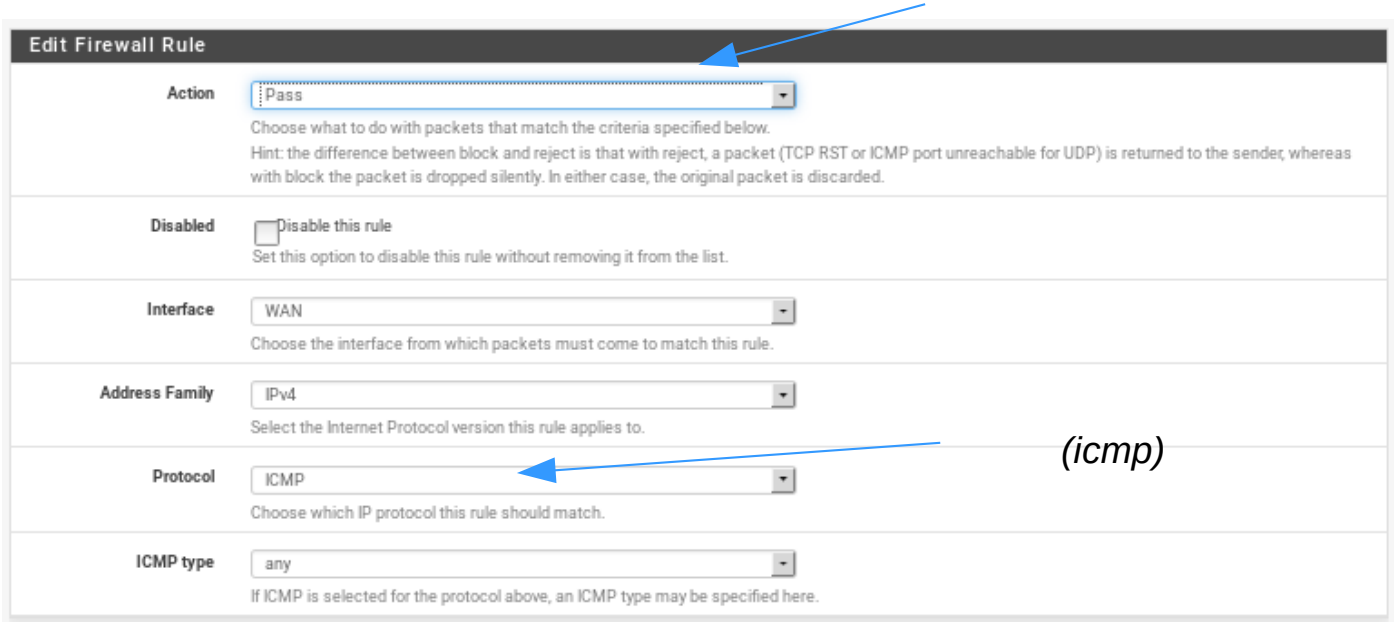
1) Wan



2) Add

Autorisée l' ICMP sur le Wan

(Action)

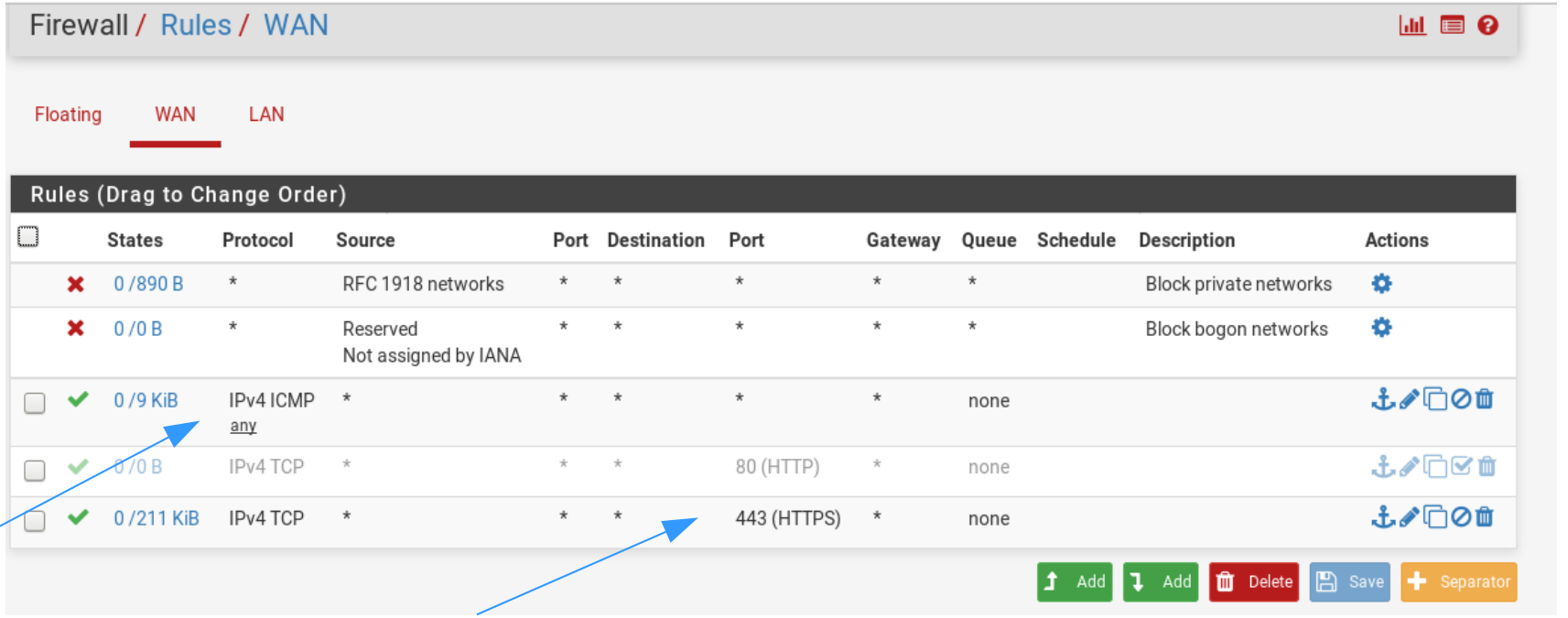


(icmp)

Menu

Firewall/Rules/WAN

Exemples de Règles pour le WAN



(icmp)

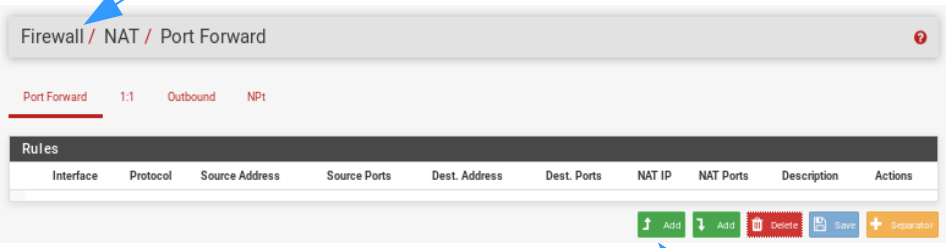
Autorisée l’accès à l’interface de gestion (Wan)

PFSENSE

Menu

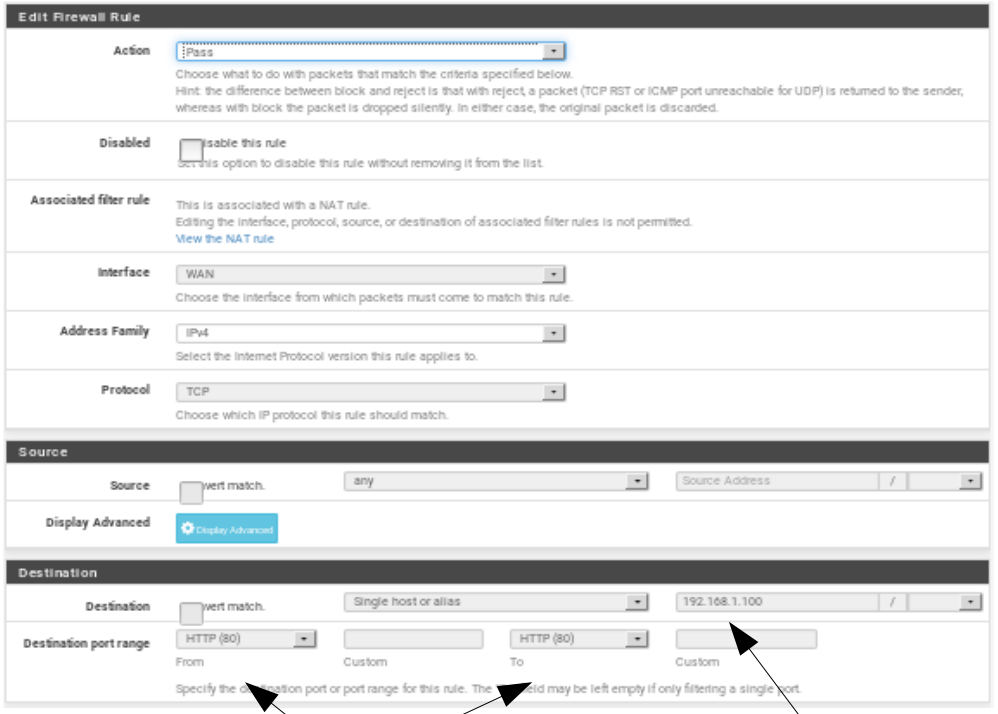
Firewall/NAT/Portforward

1) Port Forward



2) Add

Redirection du Port 80

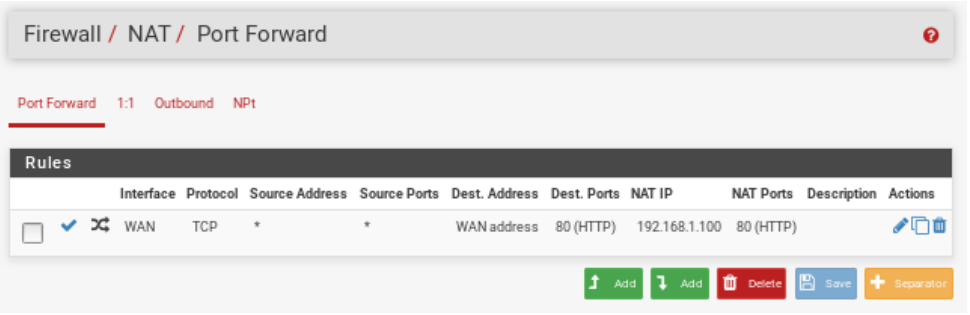


Port 80

Ip (local)

Redirection

du Wan Port 80 vers un Port 80 sur un Serveur Local



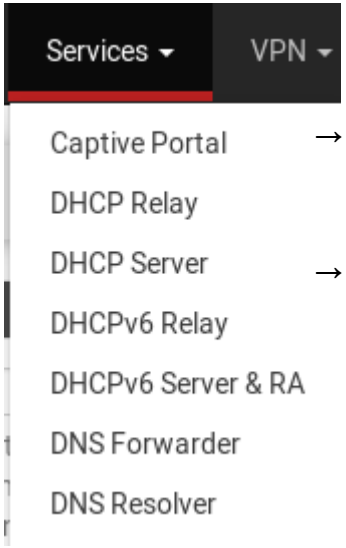
Menu FailOver

Lan Wan

Menu

Services

Service permet de configurer les différents service ainsi que les pluggins (que vous pouvez installer)



→ **Captive Portal** — Gère les accès internet

→ **DHCP Server** — Configuration du service DHCP

Menu

Services/DHCP Server/Lan

Pfsense peut être utilisé comme serveur DHCP ou relai DHCP

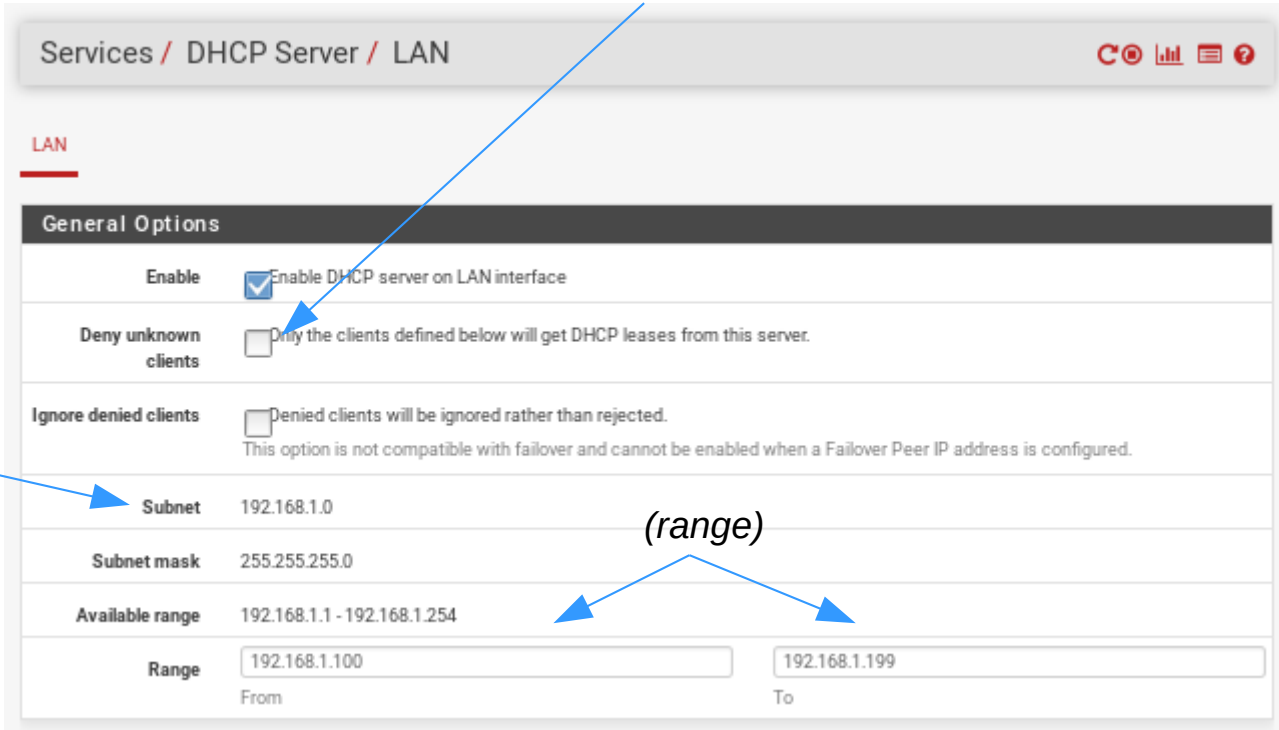
Configuration :

en tant que serveur DHCP

(deny) Autorisation par adresse Mac

(réseau)

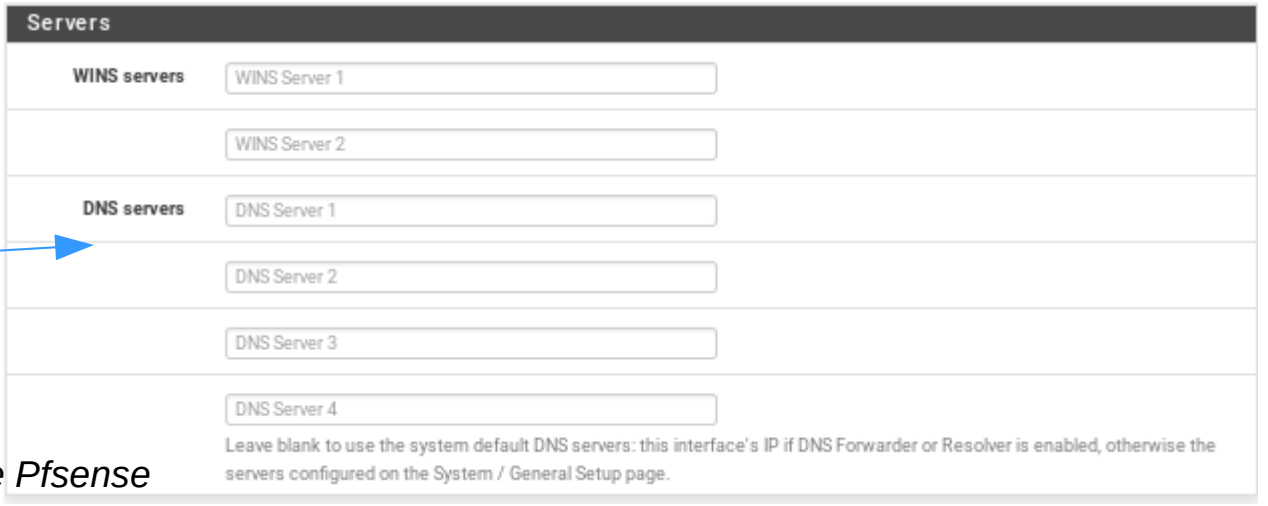
(range)



Menu

Services/DHCP Server/Lan

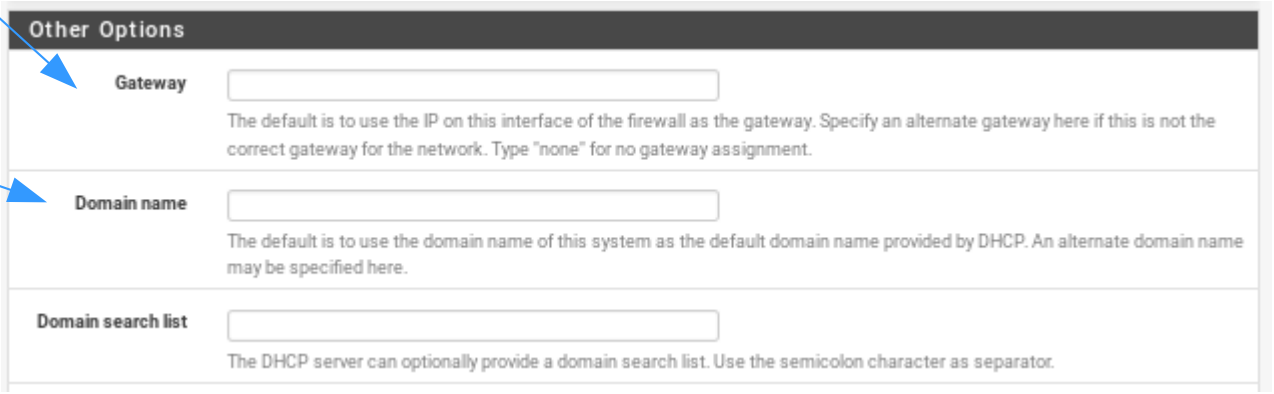
Option WINS/DNS



(DNS servers)
vide pour utilisé ceux de Pfsense
Si vous avez AD indiquer l'adresse

(Gateway)
vide pour utilisé ceux de Pfsense

(Domain name)
Nom FQDN



Menu

Services/DHCP Server/Lan

Option WINS/DNS

(Failover peer IP)
Si vous avez 2 Pfsense

(Dynamic DNS)
Serveur DNS dynamique

(Mac Adresse Control)
Filtre les accès au DHCP par adresses MAC

(NTP)
Serveurs de temps

(TFTP)
Serveurs TFTP pour l'approvisionnement de téléphone IP DHCP 66

(LDAP)
Serveurs LDAP

(Enable network booting)
Activer le boot network ainsi que le nom du fichier

(Additionnal Boot/DHCP options)
Ajout n'importe quelle option DHCP

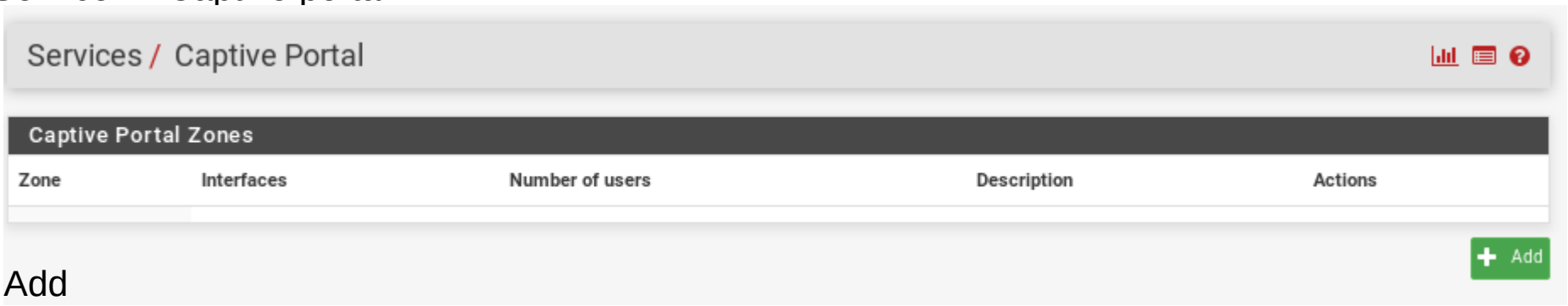
PFSENSE

Menu

Services/Captive Portal

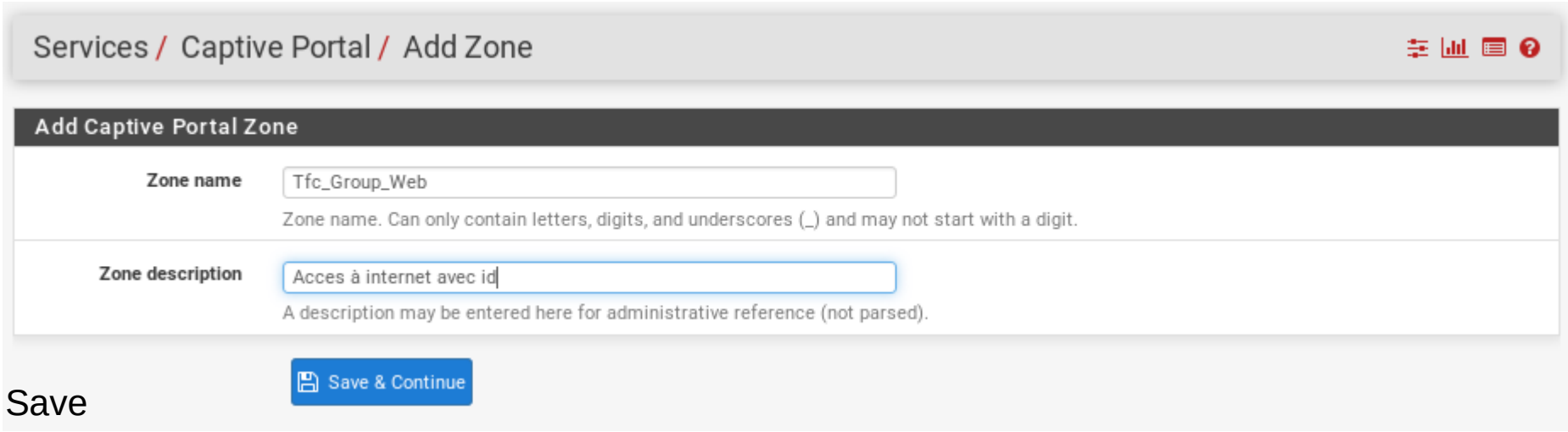
Le portail captif,permet de demander une authentification pour pouvoir accéder à internet

Service → Captive portal



Add

1) Création du Portail nom du groupe avec ca description

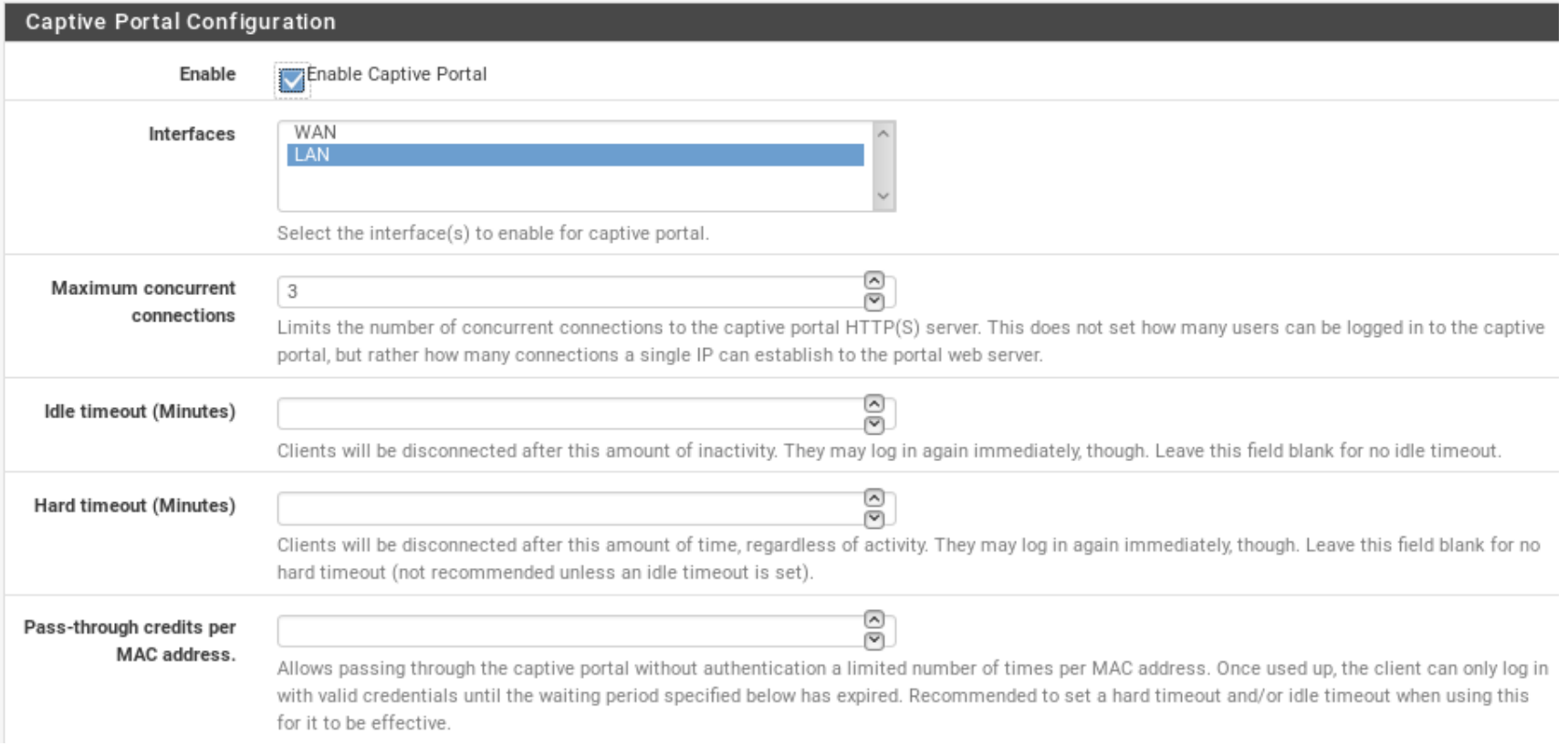


Save

Menu

Services/Captive Portal

2) Activé Portail

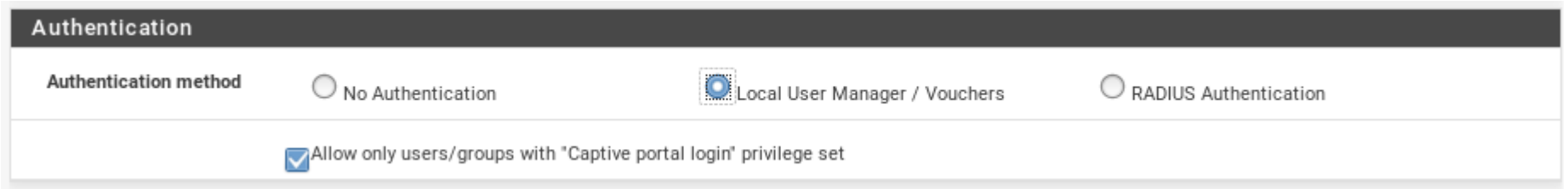


l'interface , le nbr de client

Menu

Services/Captive Portal

Authentification : local User Manager



Seul : les (users) ou (groups) avec les droits (Captive Portal login) pourront accéder à Internet

Le Captive Portal à été crée

Il ne reste plus qu'a configurer :
- Crée les utilisateurs Web

Menu
Dhcp

Services

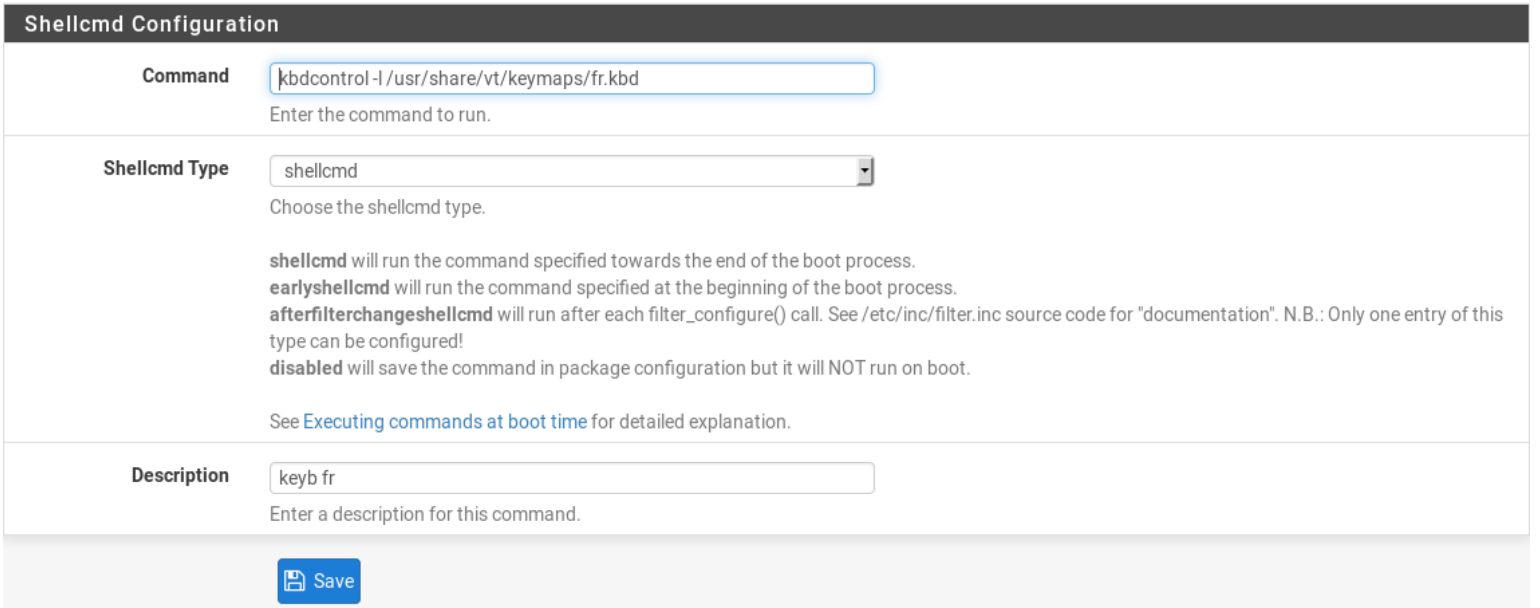
Mettre le Clavier en fr

System → Package Manager

Récupéré le pakage **Shellcmd**

Maintenant il faut le configuré :

Service → Shellcmd

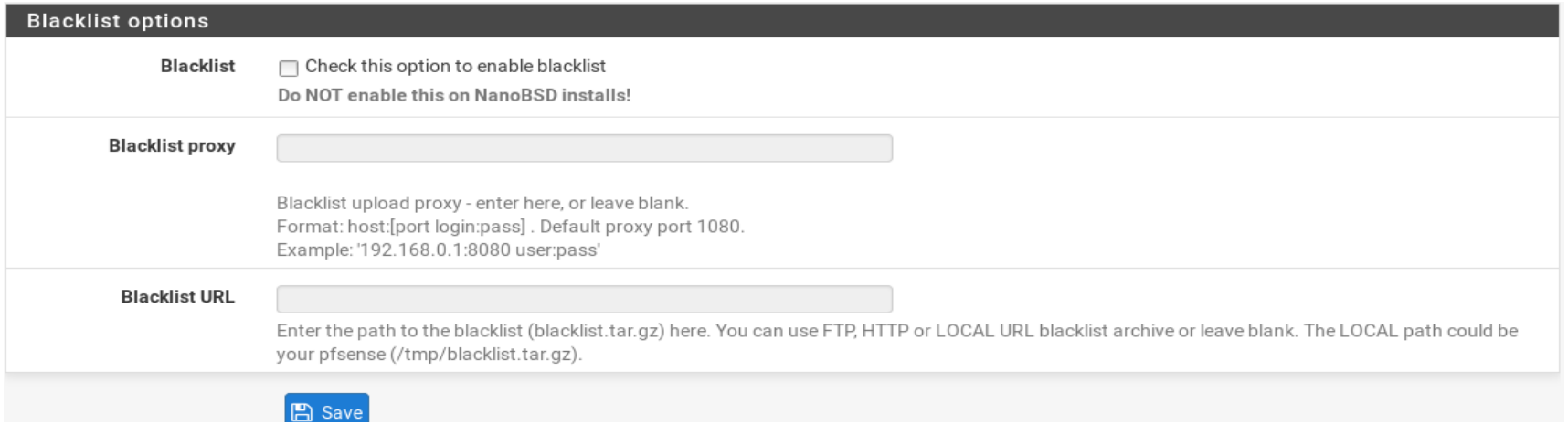


dans command : kbdcontrol -l /usr/share/vt/keymaps/fr.kbd

SquidGuard

Services → SquidGuard

Blacklist url



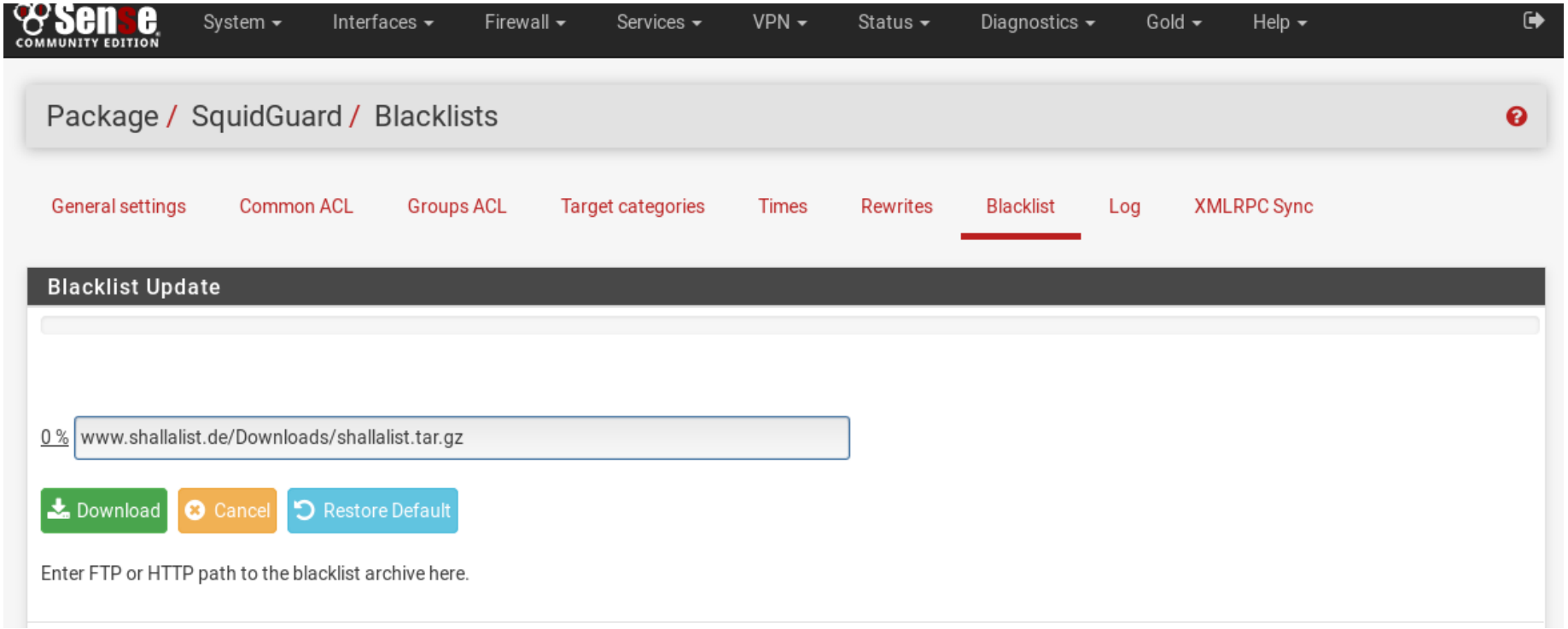
Utilisons cette blacklist dans (blacklist URL):

www.shallalist.de/Downloads/shallalist.tar.gz
http://urlblacklist.com/cgi-bin/commercialdownload.pl?type=download&file=bigblacklist
ftp://ftp.univ-tlse1.fr/blacklist/blacklists_for_pfsense.tar.gz

SquidGuard

Services → SquidGuard

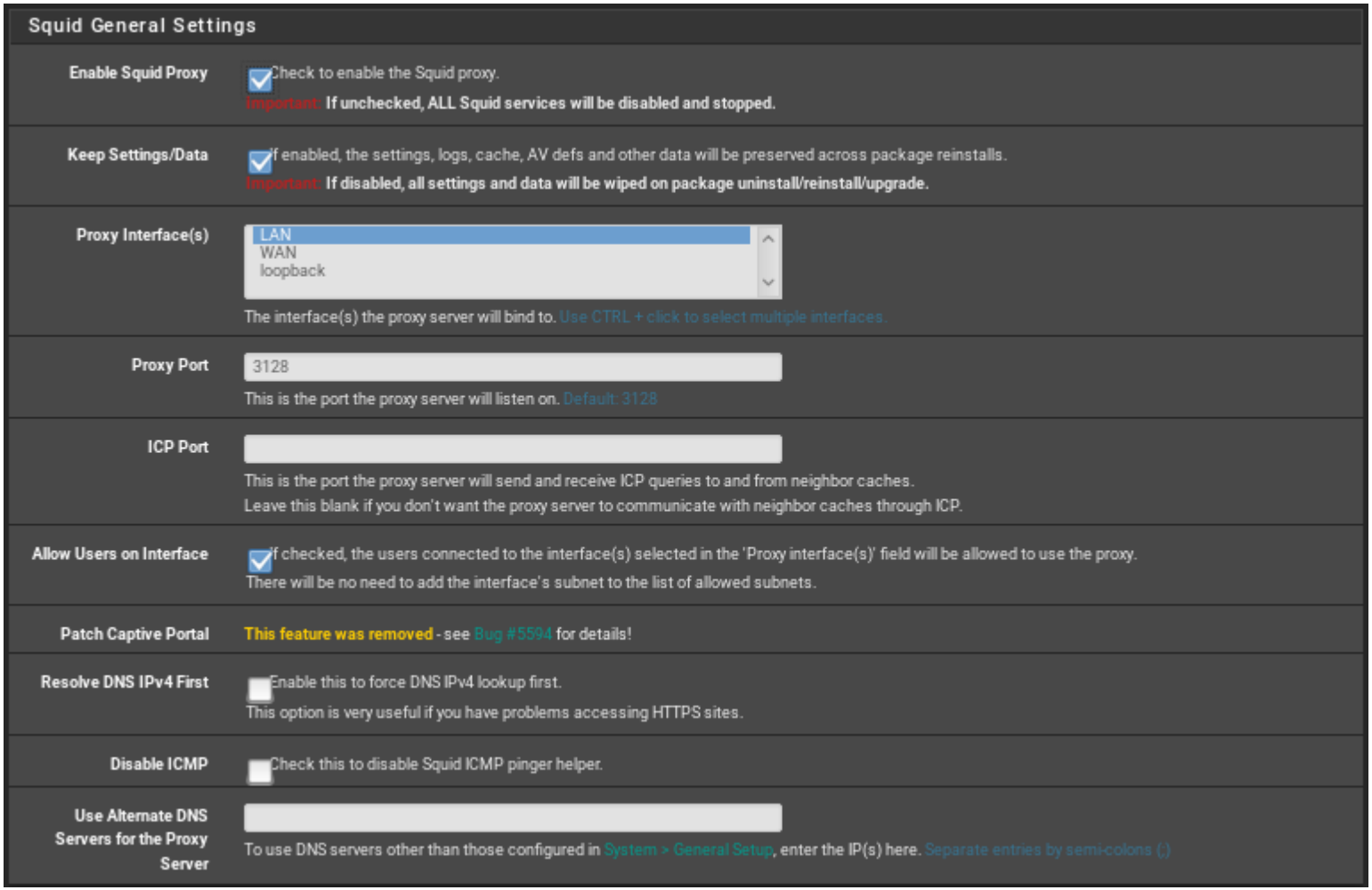
Mettre à jour la Blacklist



Proxy Server

Services → Squid Proxy Server

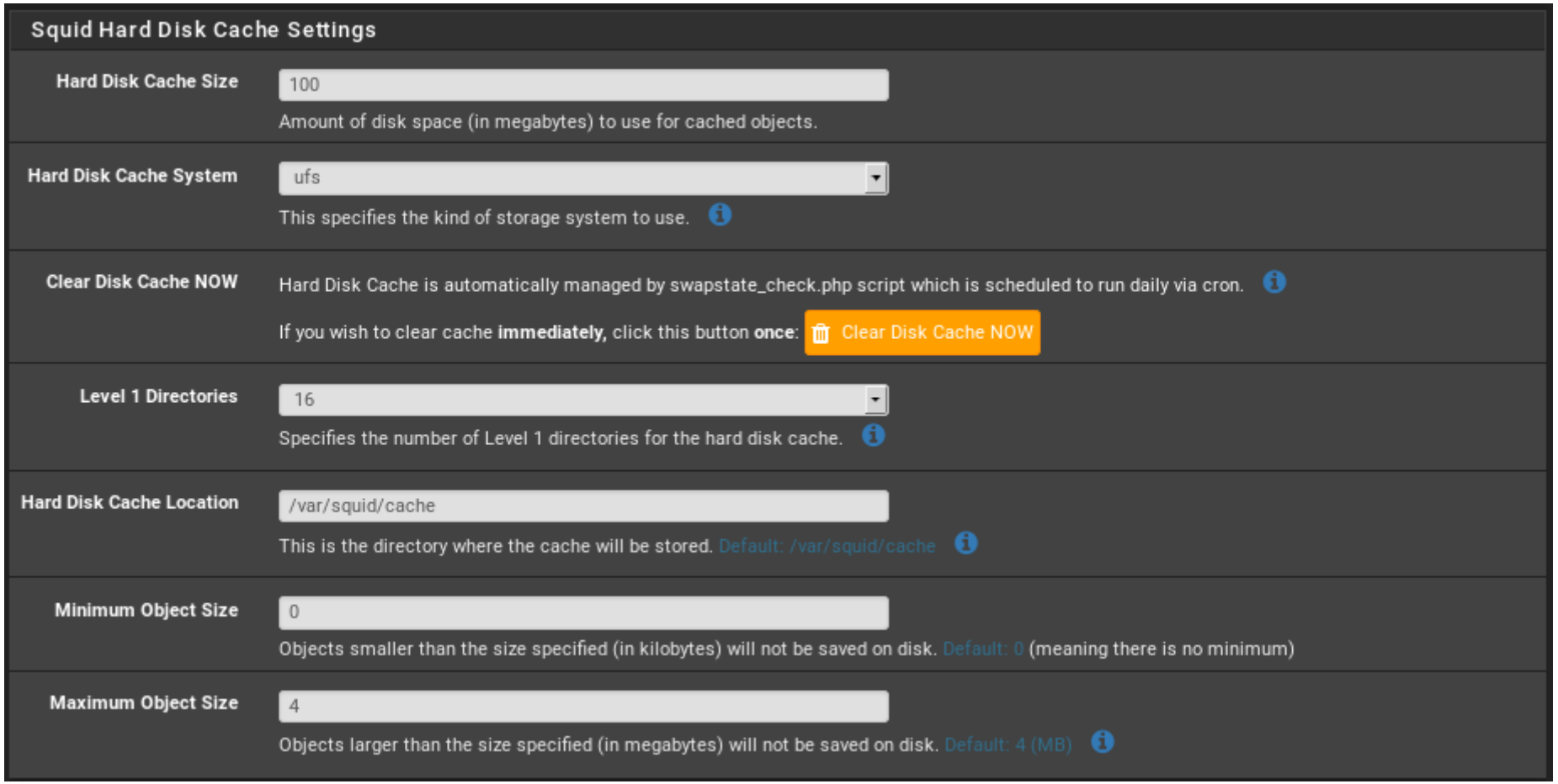
Activer le proxy



Proxy Server

si besoins Vider le cache dans

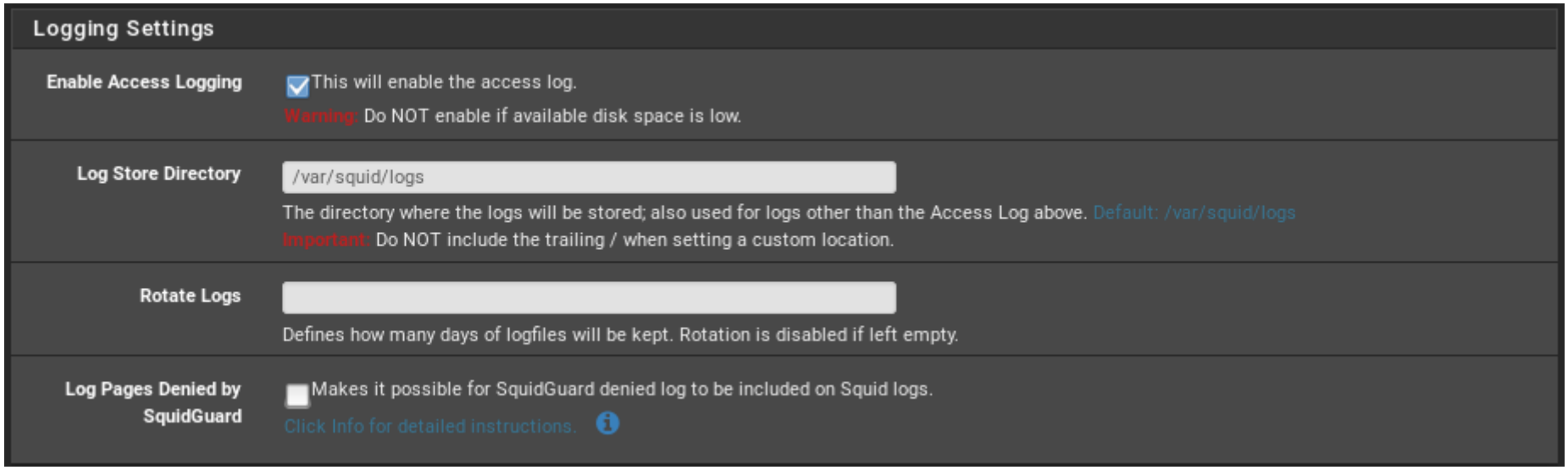
Services → Squid Proxy Server Local Cache



Proxy Server

Services → Squid Proxy Server

Activer les logs

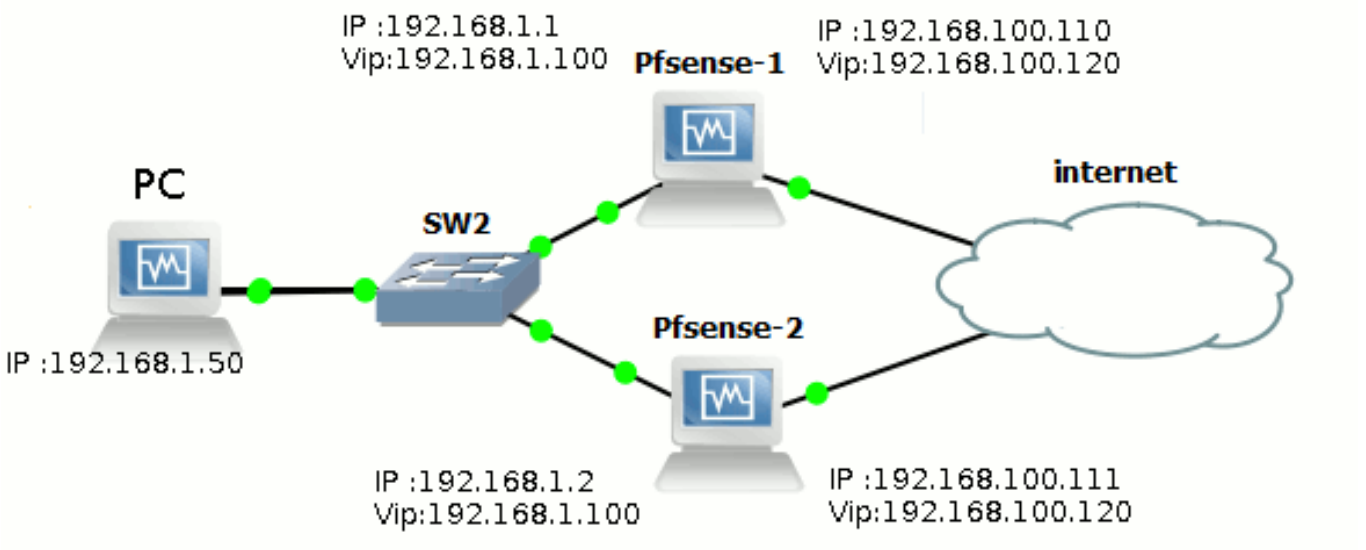


Page d'erreur Web
/usr/local/www/sgerror.php

Menu

Firewall/Virtual IPs

2 Pfsense redondants,permet d'avoir 2 Routeurs pour l'équilibrage de charge ou en cas d'une défaillance de l'un

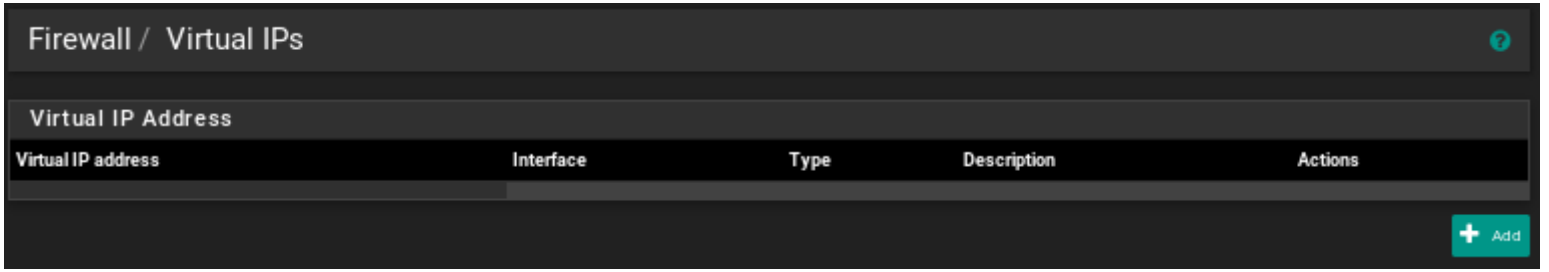


CARP (Common Adress Redundancy Protocol) est un protocol permettant à plusieurs hôtes de partager une adresse IP
Pfsync est protocol permettant de synchroniser entre deux serveurs l'état des connexions en cours.
Il est recommandée d'utilisée une IP dédié ou LAN
XML-RPC est un protocol permettant la réplication de données d'un serveur vers un autres

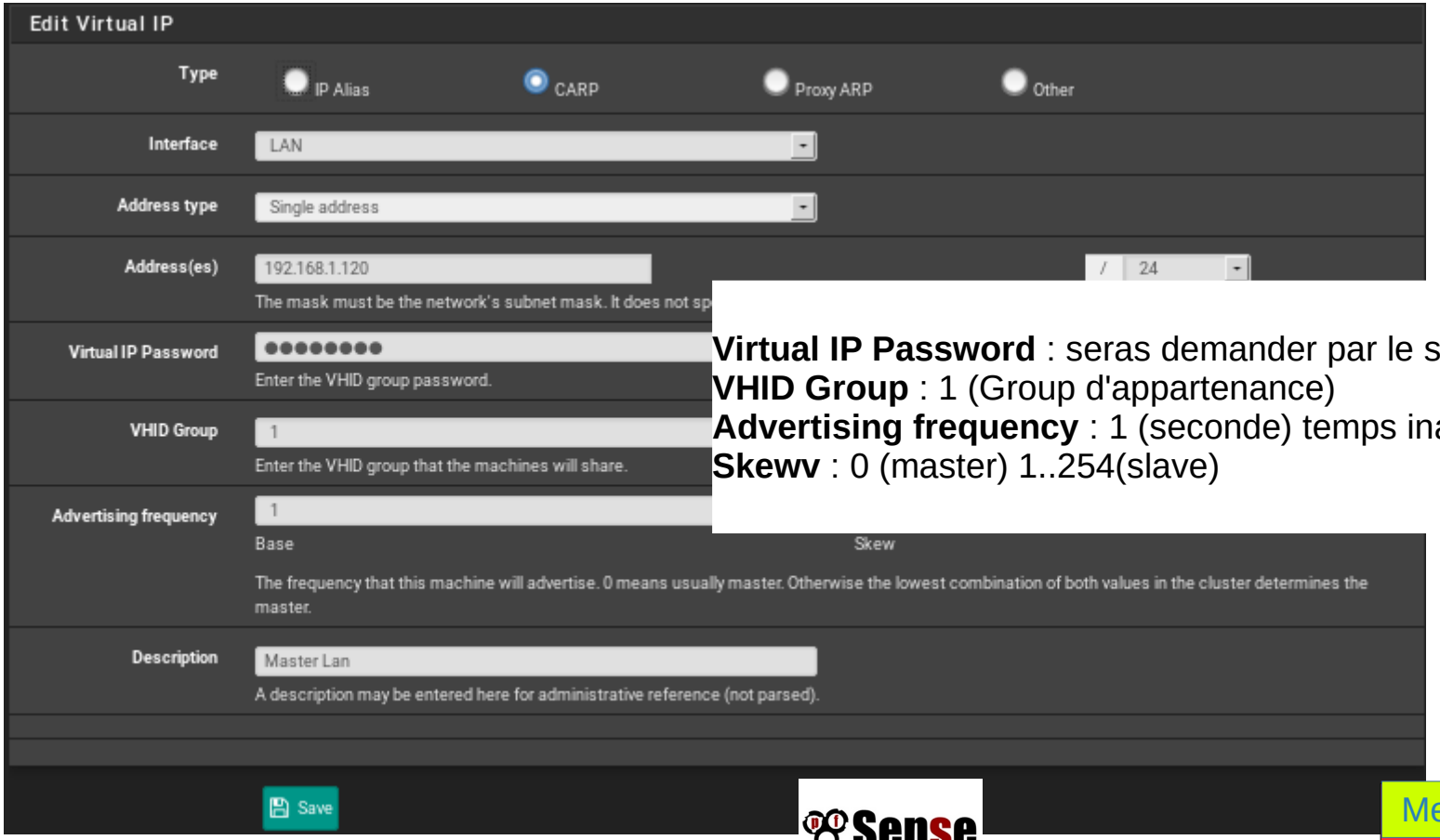
PFSENSE

Firewall/Virtual IPs

1) Création de notre IP Virtuel



2) Add



Virtual IP Password : seras demander par le serveur secondaire
VHID Group : 1 (Group d'appartenance)
Advertising frequency : 1 (seconde) temps inactivité avent de basculé
Skewv : 0 (master) 1..254(slave)

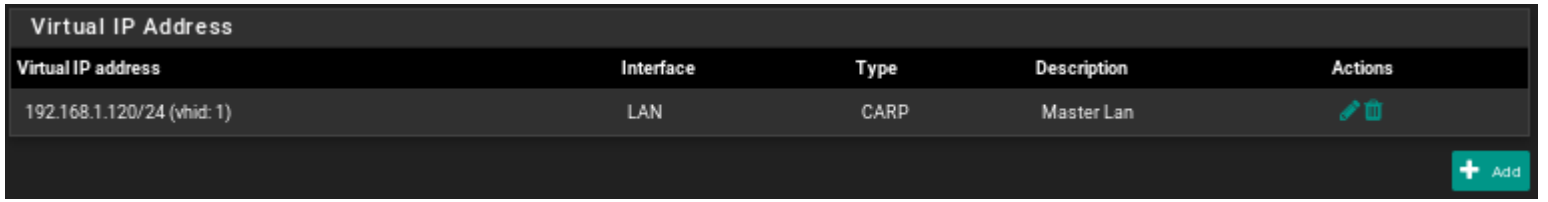
Menu

Menu
Lan
Wan
PortForward

PFSENSE

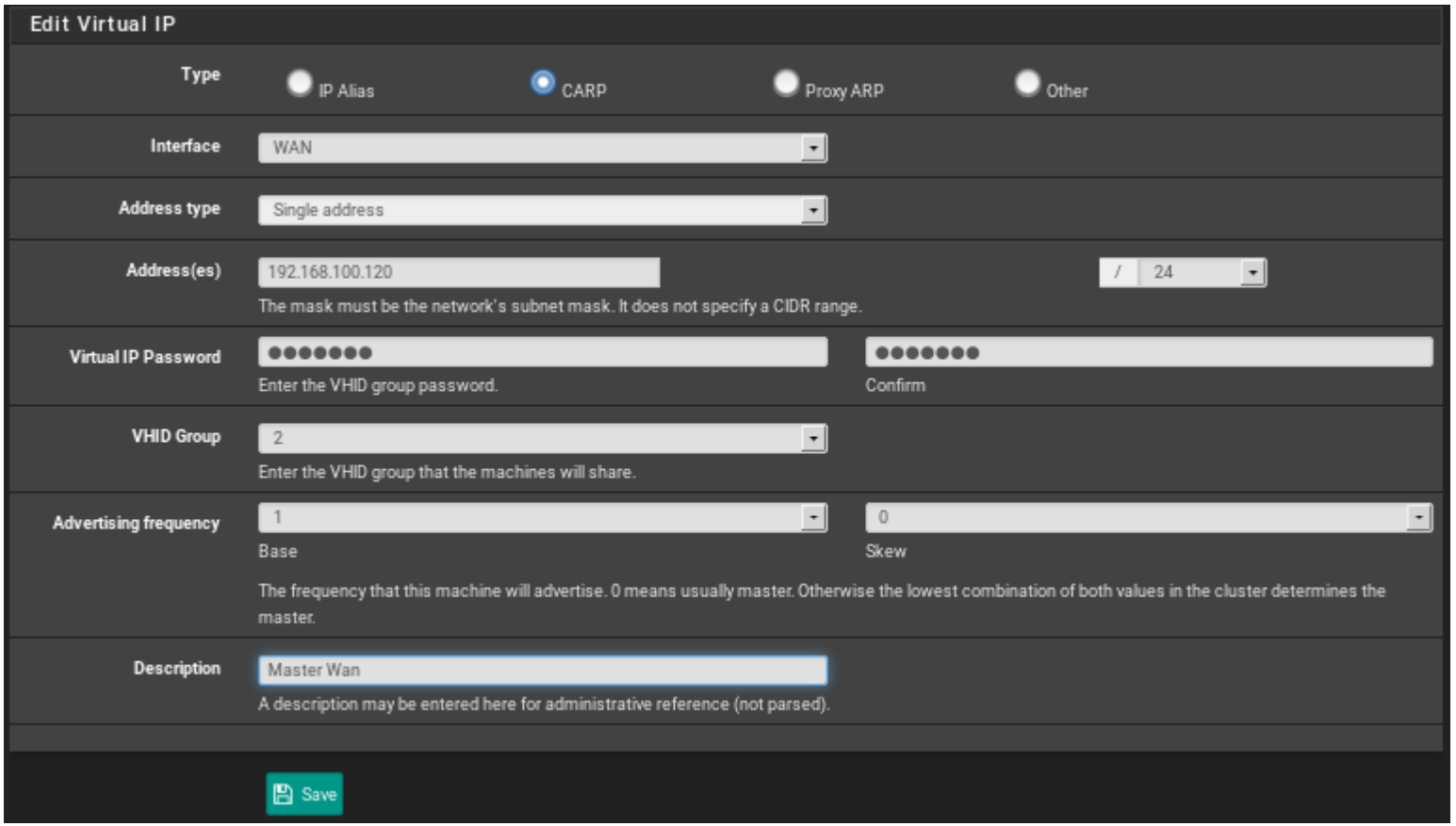
Firewall/Virtual IPs

Le LAN est crée



Add

Pour le WAN



Save

Menu

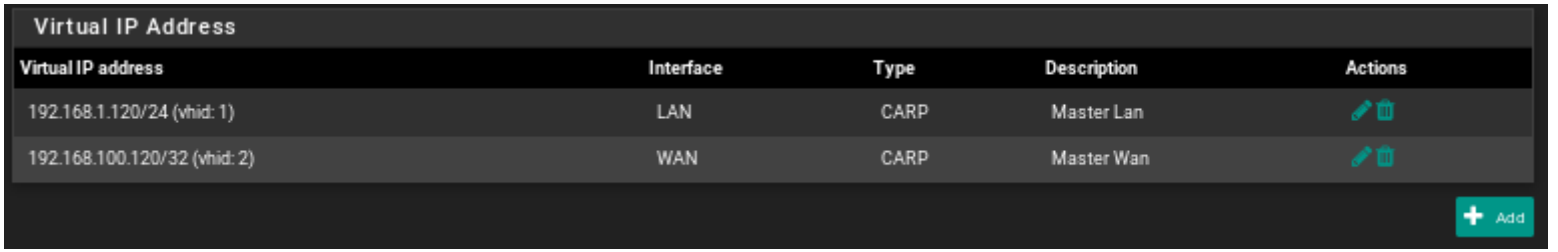
Menu

Lan | Wan | PortForward

PFSENSE

Firewall/Virtual IPs

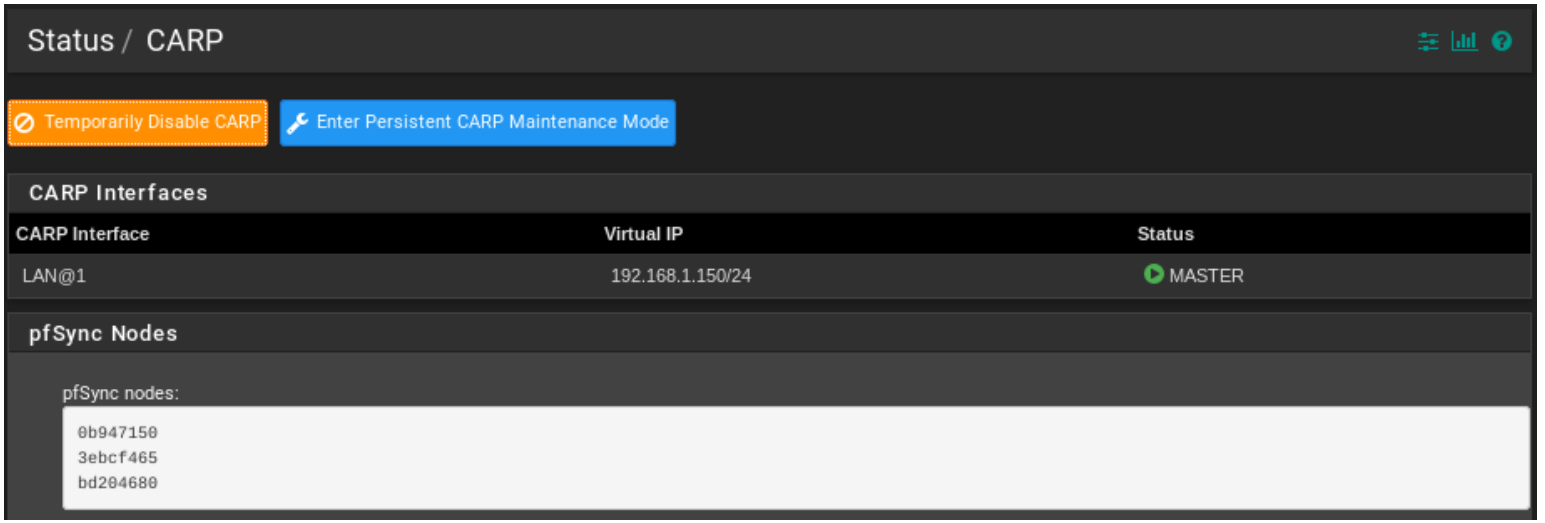
Le WAN et le LAN sont crée



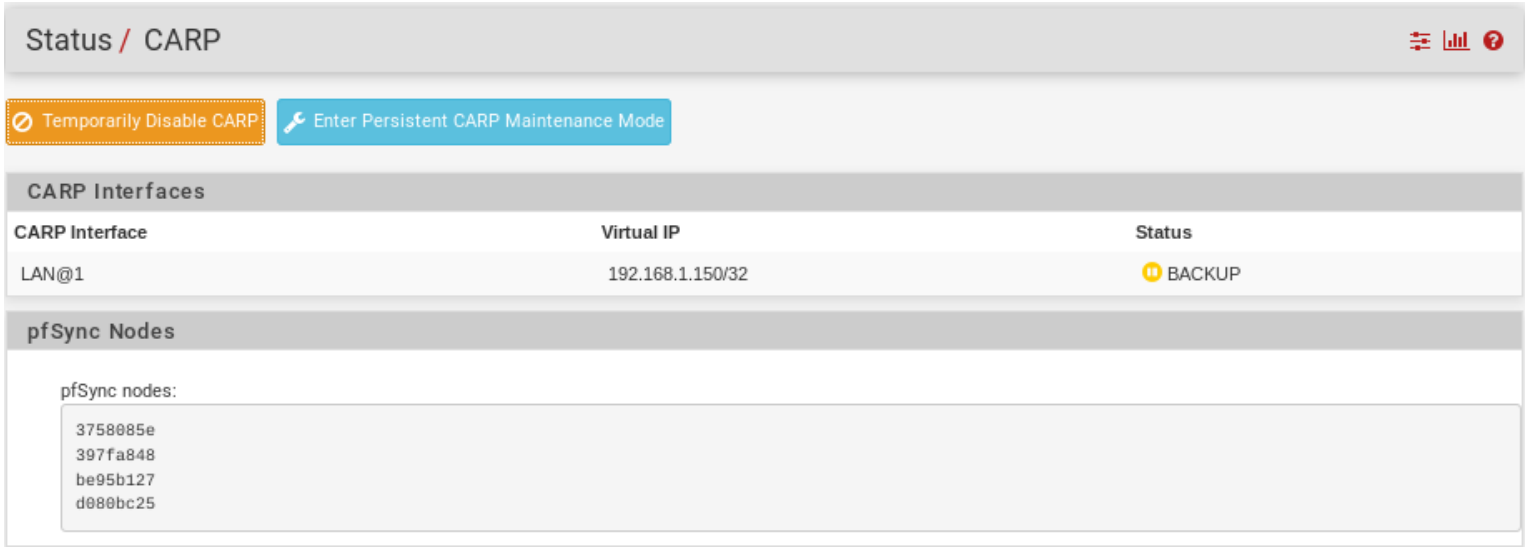
Des que vous avec configuré les Serveurs

Nous allons vérifier l'état de nos IP Virtuelles

Status → CARP (failover)



Sur le Serveur n°1 (master)



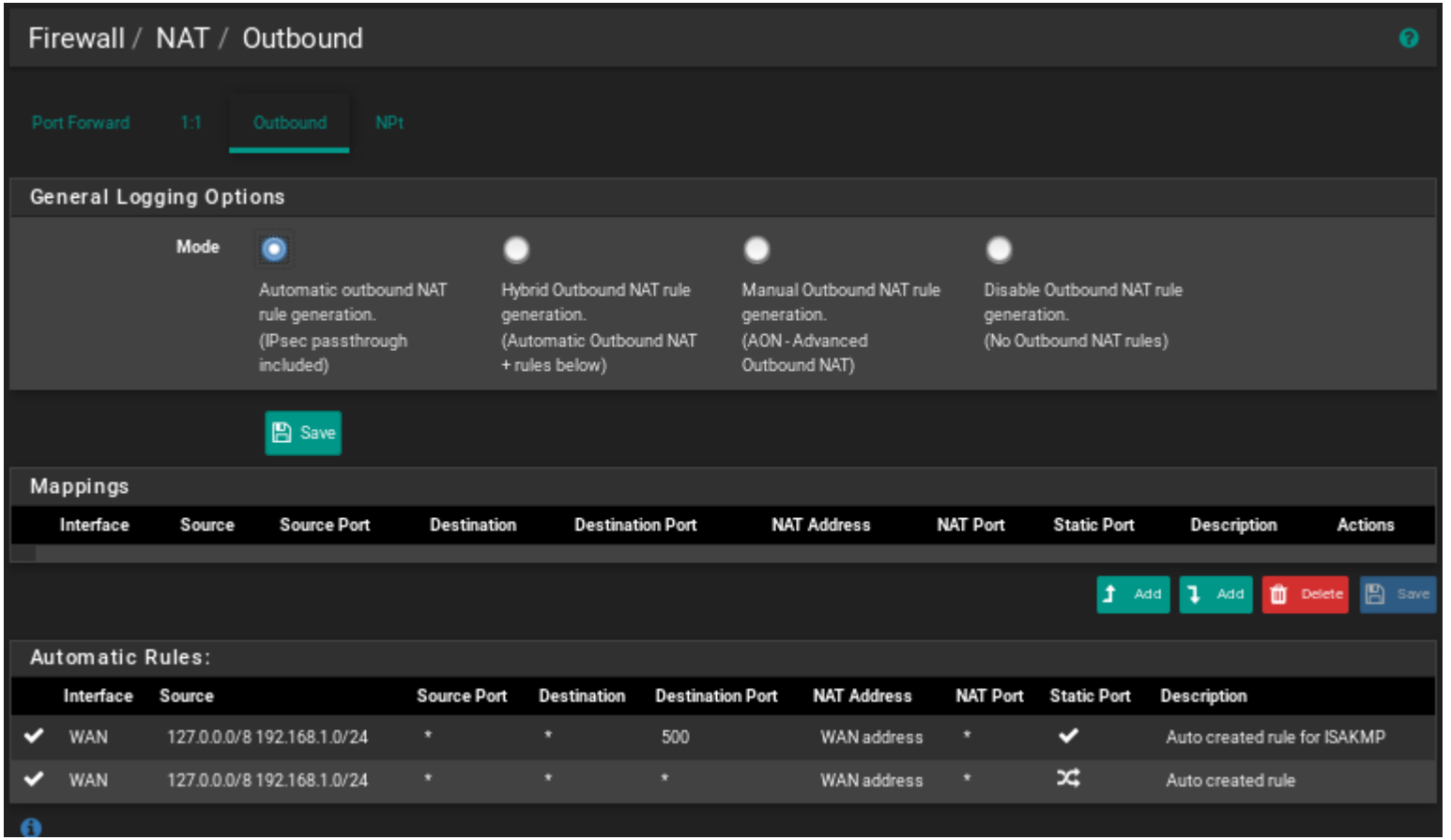
Sur le Serveur n°2 (slave)

Menu
Lan
Wan
PortForward

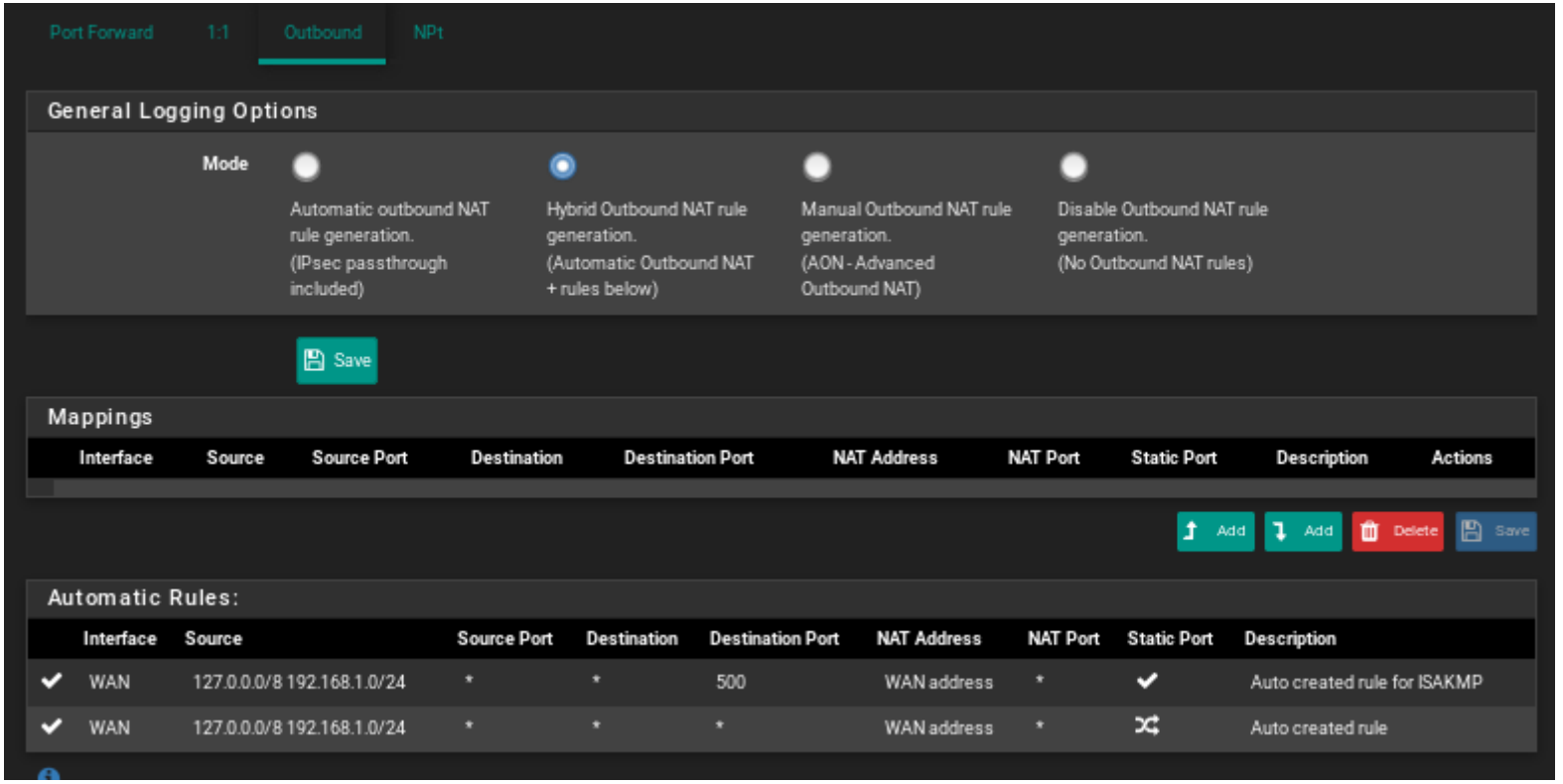
Création de l'IP Virtuel réussi

Il faut que les clients maintenant point sur l'IP 192.168.1.150

Firewall → Nat Nous modifions la règles de firewall



Pour passer à :
Hybrid Outbound NAT rule generation.(Automatic Outbound NAT + rules below)

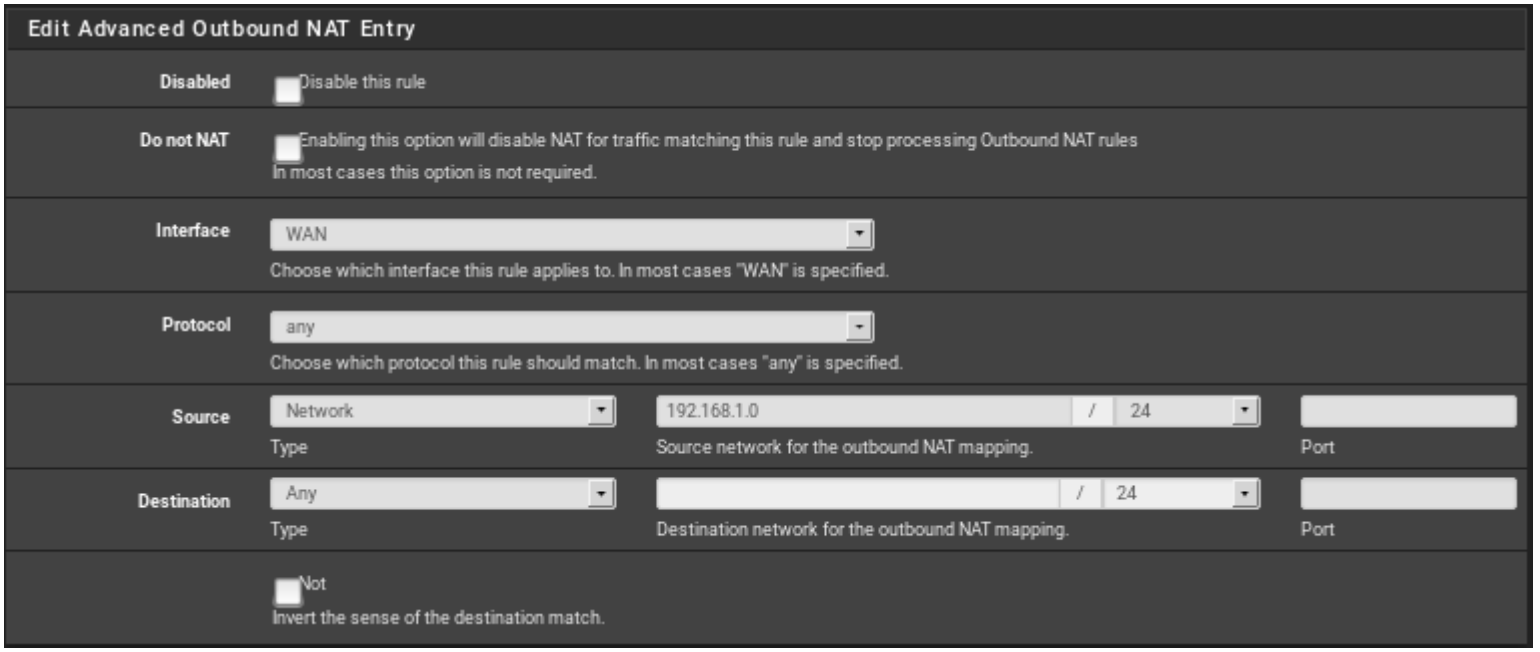


Save
Add

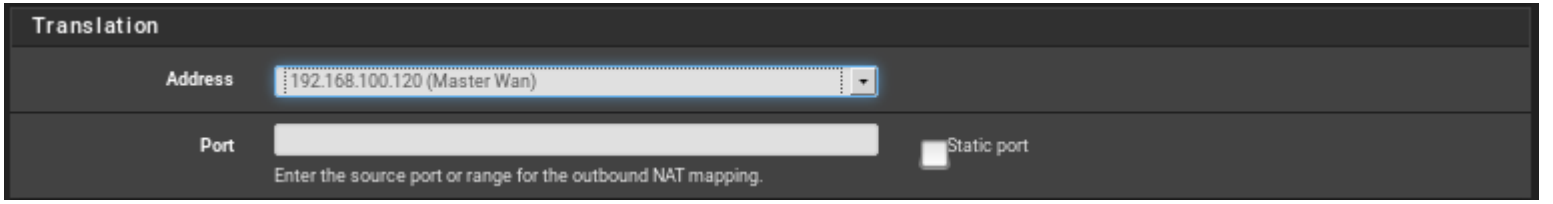
Menu
Lan Wan PortForward

PFSENSE

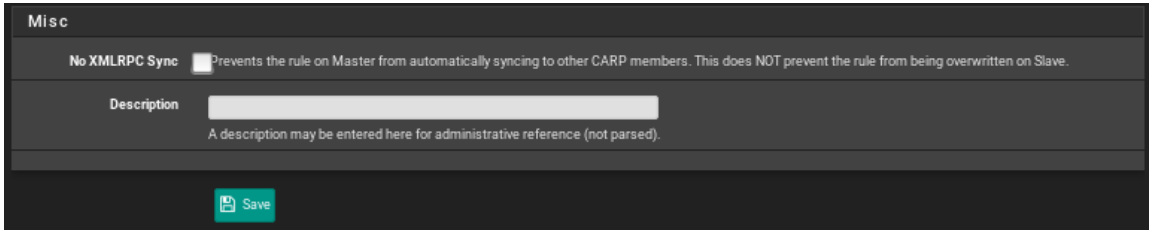
Pour l'interface WAN



Source Notre réseaux LAN



Adress Notre IP WAN



Save

Menu

Menu

Lan | Wan | PortForward

Création du NAT réussi

Modifier le DHCP pour prendre en compte en Gateway notre VIP 192.168.1.120

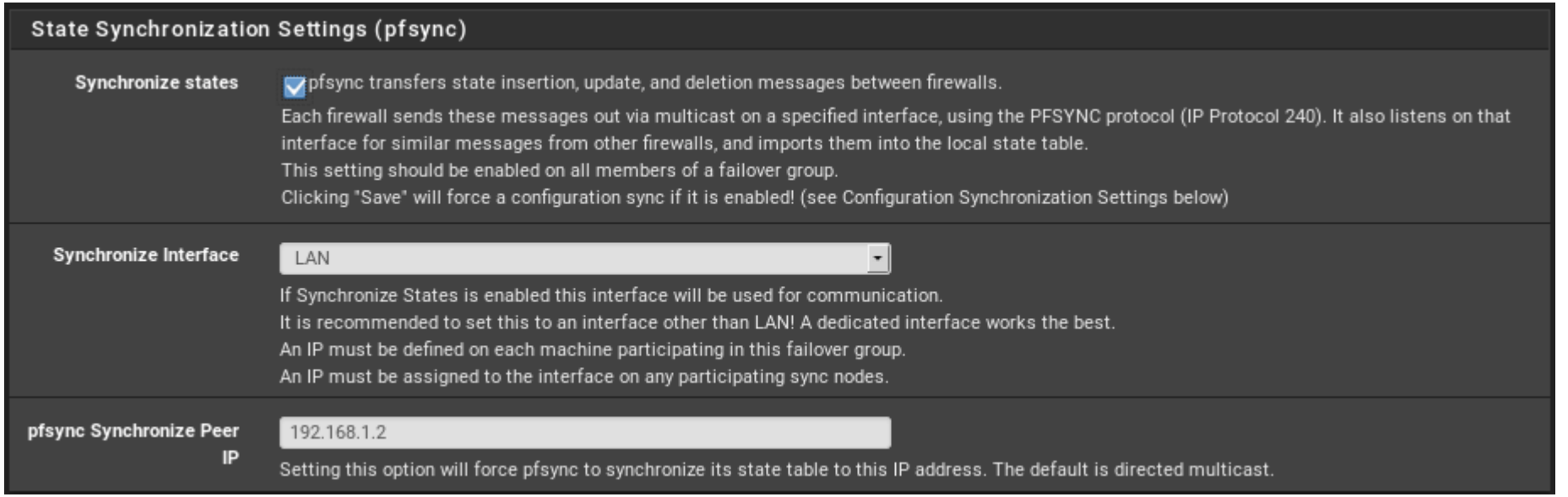
Services → DHCP Server

Failover peer IP (Optionnelle) permet de partager le lease DHCP, si le champs est renseigner vous devez modifier sur Pfsense secondaire la valeur (skew) qui doit être supérieur à 20

Création du DHCP réussi

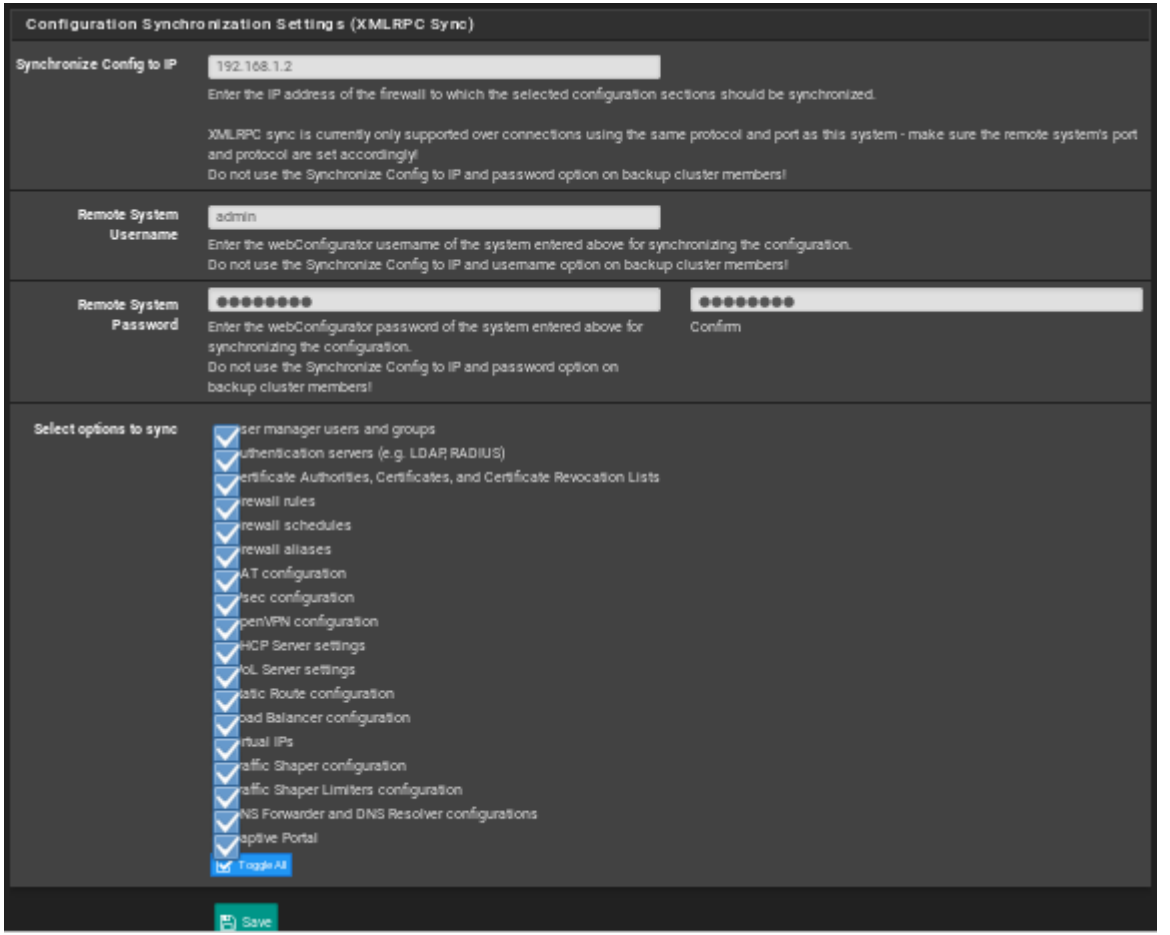
Modifier OpenVpn pour prendre en compte en Gateway notre VIP 192.168.1.120

System → High Avail. Sync



Synchronize states : Cocher la case pour activer la synchronisation
pfsync Synchronize Peer IP : Ip du serveur de secours (LAN)

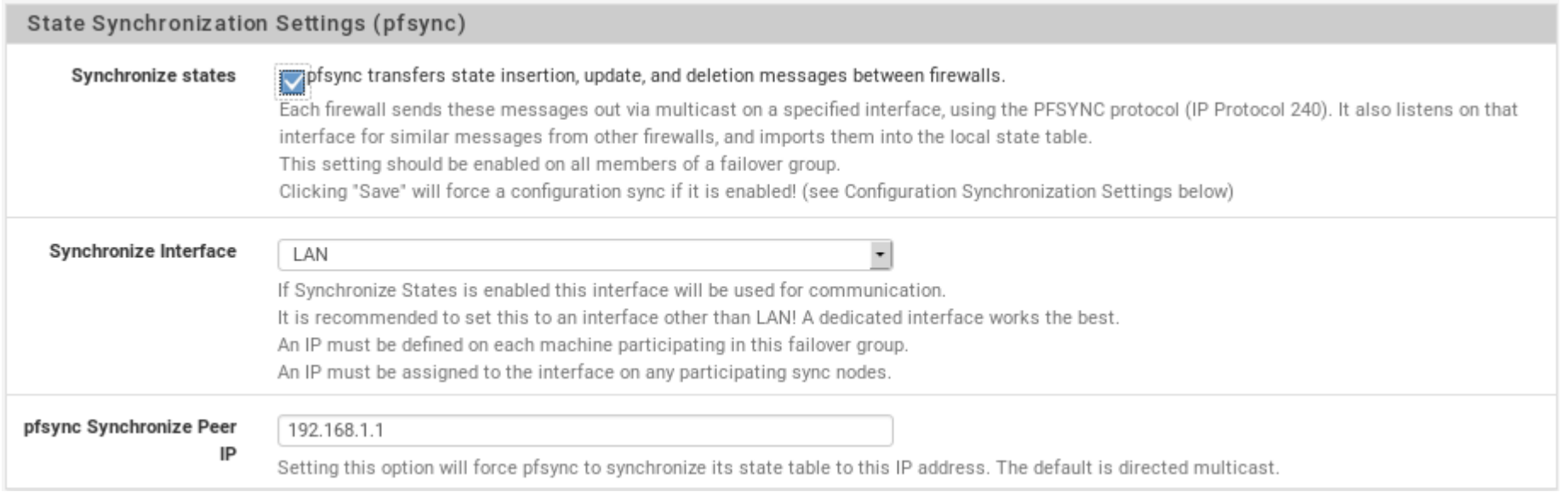
Config de : XMLRPC Sync



Synchronize Config to IP : Ip du serveur de secours (LAN)
Remote System Username : saisir un compte avec paswword
Select options to sync : Sélectionnée les services a synchroniser sur le serveur de secour

Menu
Lan
Wan
PortForward

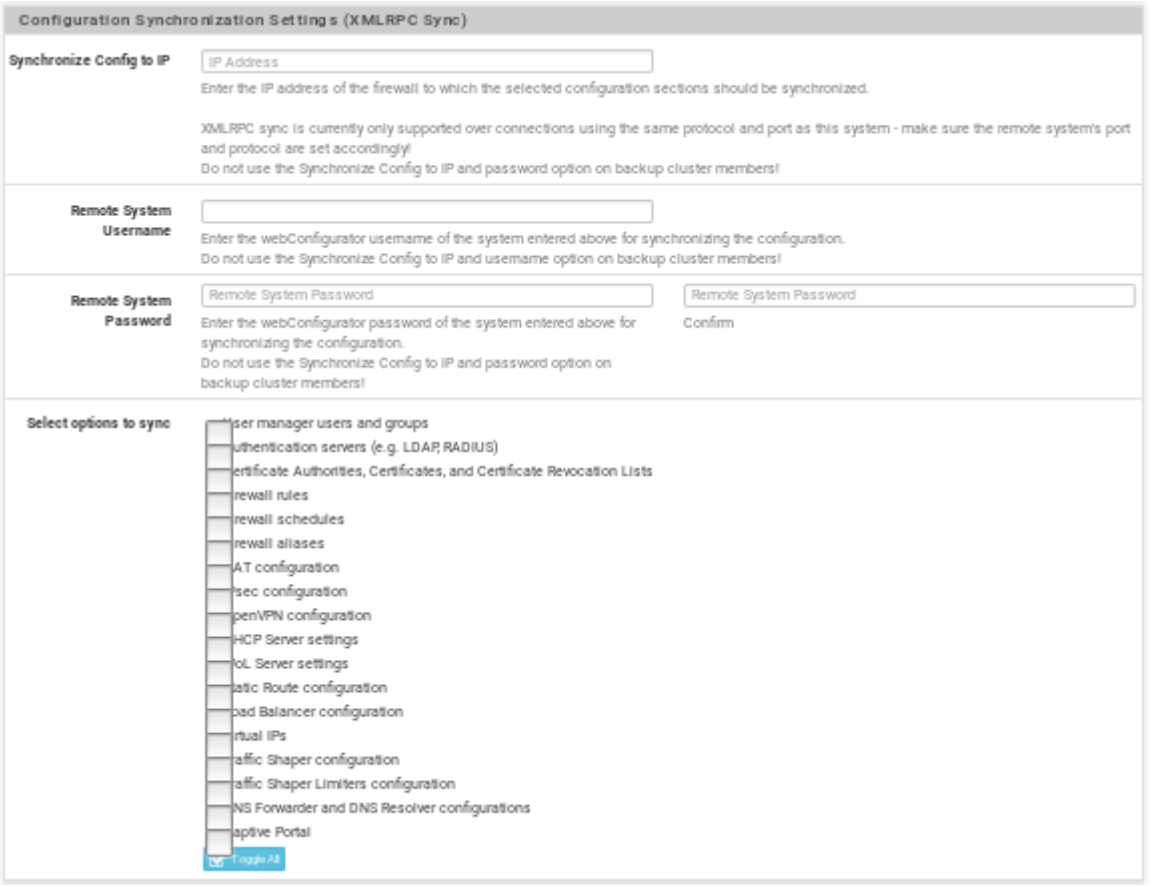
Sur le Serveur Secondaire



Synchronize Config to IP : (Optionnelle) Ip du serveur Maitre (LAN)

Menu
Lan
Wan
PortForward

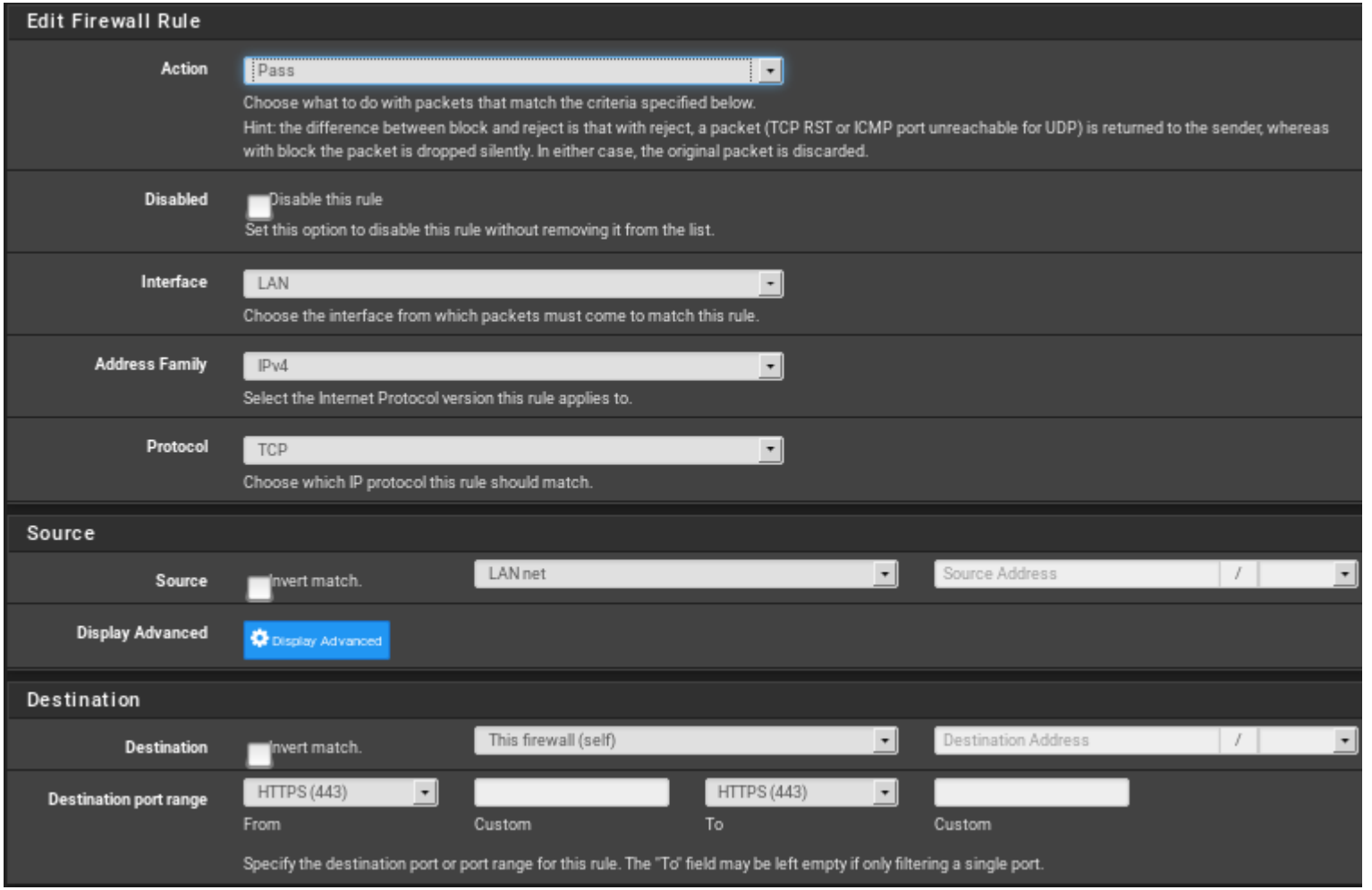
Config de : XMLRPC Sync



Rien a indiquer à partir de maintenant la synchronisation devrait fonctionner

Autoriser le flux sur le firewall

Si le port https n'est pas ouvert, vous pouvez lui attribué une regles



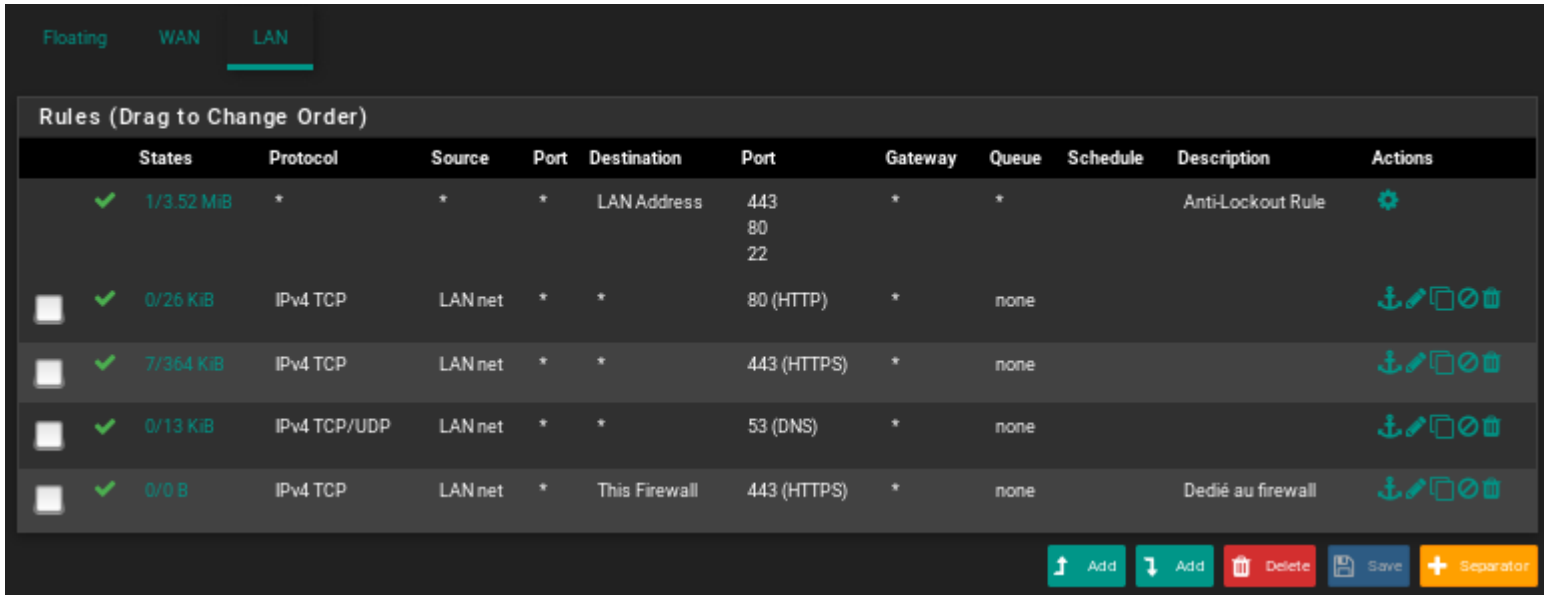
Save

Menu

Menu

Lan | Wan | PortForward

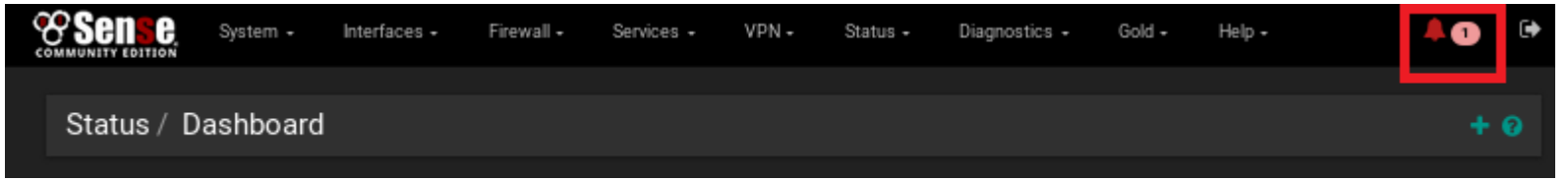
La nouvelle règles est :



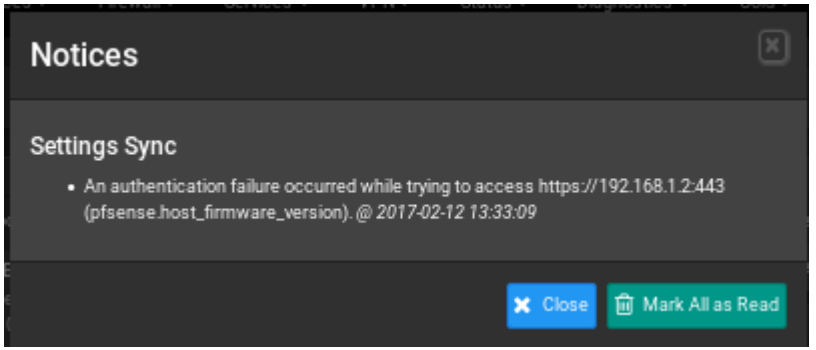
Autorisation du flux réussi

Voir les erreurs

Si une erreur est trouvé par Pfsense



clicker sur la cloche



Ici le message indique qui il y as sans-doutes une erreur avec le mot de passe ou le compte utilisateur

Faites des testes
- Redémarré le serveur, débrancher le câble réseaux pour vérifier que le primaire devient bien master