PROJET : Cluster pfSense HA (Haute Disponibilité)

Le matériel nécessaire : 2 routeurs pfSense et deux machines clientes sous Windows 10 ou 11.

Les ressources indispensables pour installer correctement nos pfSense : 2 Gio de RAM, trois cartes réseau (WAN, LAN, SYNC). Il faut effectuer la même configuration sur le second pfSense. Prévoir également 10 Go de disque dur et 2 CPU.

L'objectif de ce TP est d'assurer la redondance entre deux pfSense, de réaliser la synchronisation entre le master et le backup, et de configurer une VIP (IP virtuelle) afin de garantir une **disponibilité constante des services et une transparence pour l'utilisateur.**

MASTER	**BACKUP**
10.10.11.168(WAN)	**10.10.11.16G(WAN)**
172.16.1.10(LAN)	**172.16.1.11(LAN)**

La console principale de pfSense (Master)

La console du Backup après les modifications indispensables : désactivation du pare-feu et attribution d'une adresse IP statique à l'interface LAN.

Pour désactiver le pare-feu de pfSense : appuyer sur 8 pour entrer dans le shell, puis taper « pfctl -d ». Pour le relancer, utiliser « pfctl -e ».

Lorsque vous désactivez le pare-feu, celui-ci se relance à chaque modification de configuration que vous effectuez. Afin de le maintenir éteint, vous pouvez utiliser la commande suivante qui le désactive en boucle :

sh -c 'while true; do pfctl -d; sleep 5; done'

Pour revenir à l'interface de pfSense, il faut sortir du shell :

exit

Astuce :

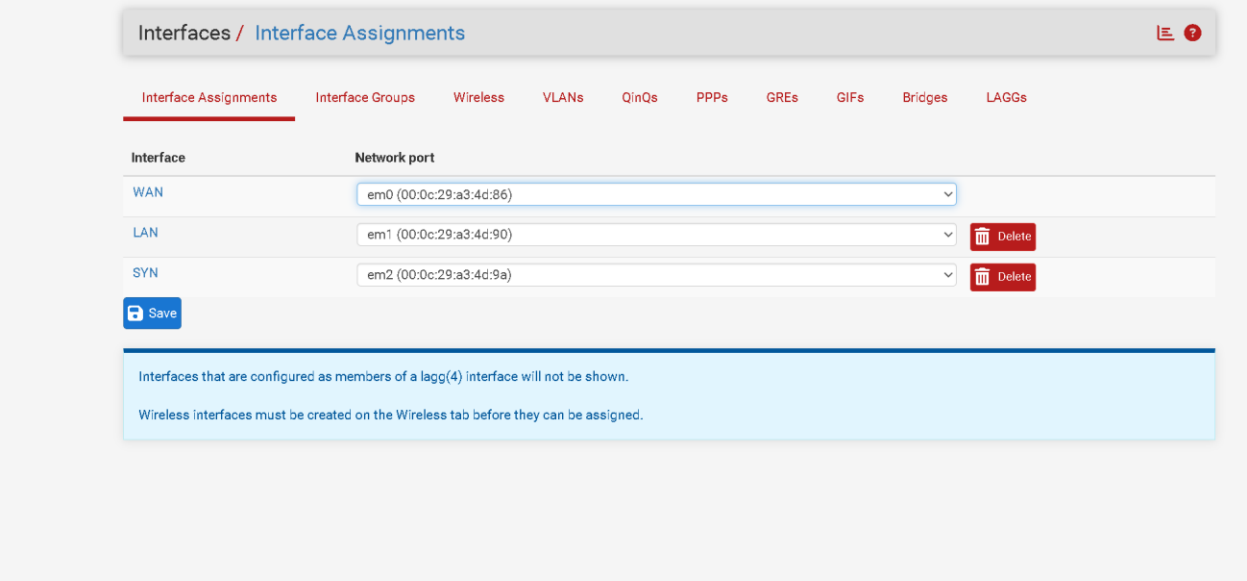
DEBUG :

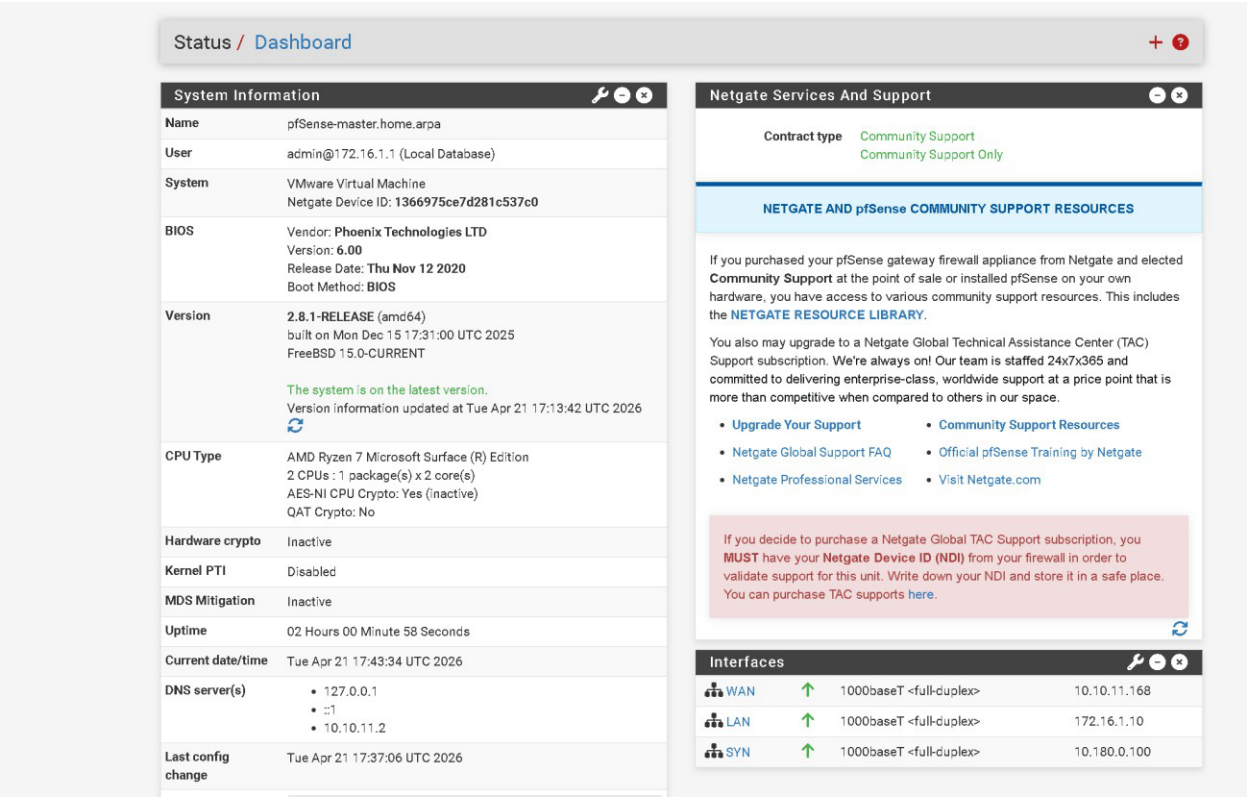
Si votre clavier n'est pas en français et que vous avez du mal à trouver certains caractères (notamment le « - »), copiez/collez la commande dans la VM en utilisant la fonctionnalité « coller » de VMware :

Menu VMware : Edit > Paste

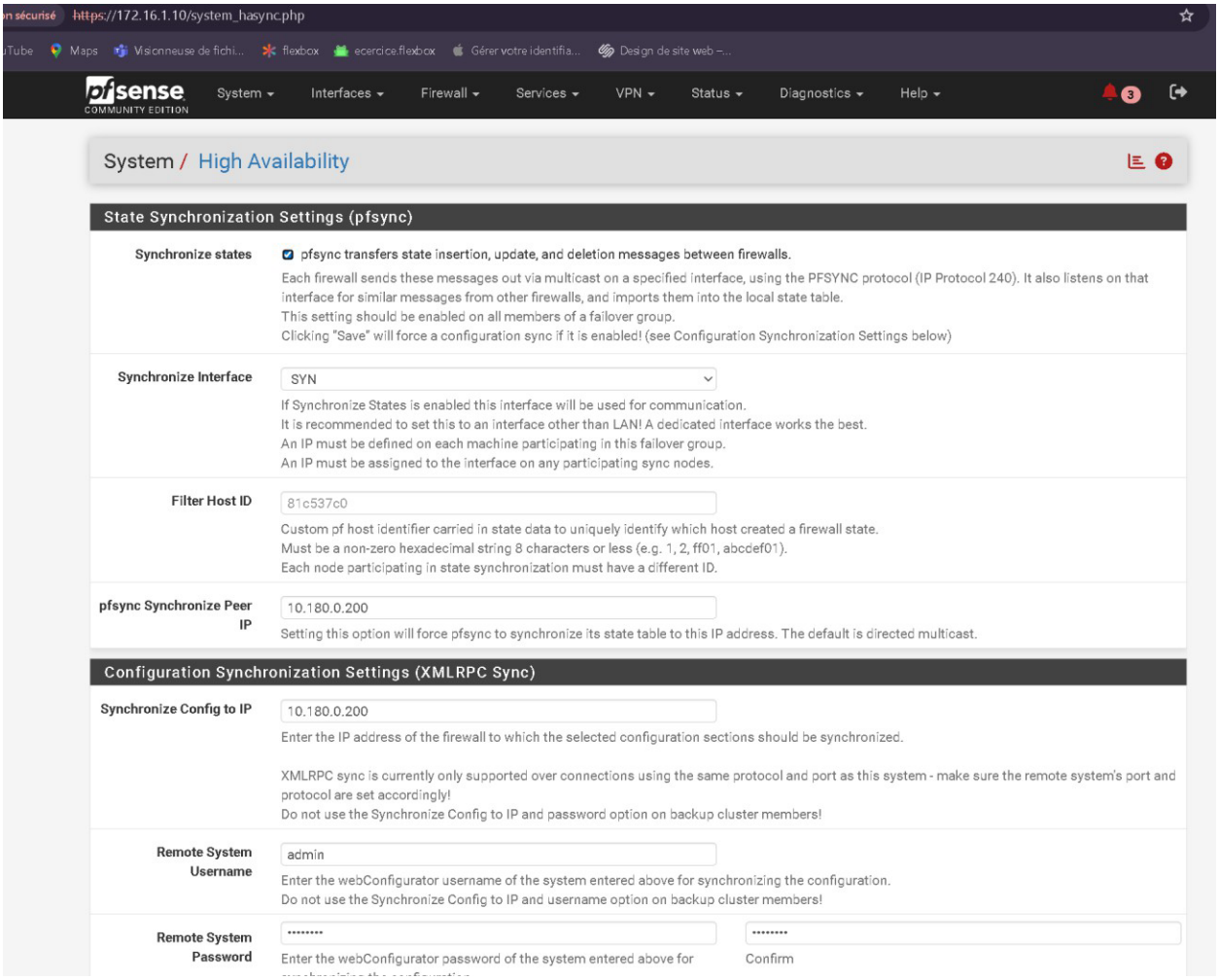
Pour pouvoir mettre en œuvre le cluster HA, il faut dans un premier temps réaliser la synchronisation avec pfsync. Pour cela, il est nécessaire d'ajouter et de dédier une carte réseau sur chacune de nos VM, ainsi qu'une plage d'adressage dédiée et spécifique :

MASTER	BACKUP
SYNC : 10.180.0.100	SYNC : 10.180.0.200


Interfaces / Interface Assignments
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (00:0c:29:a3:4d:86)
LAN
em1 (00:0c:29:a3:4d:90)
Delete
SYN
em2 (00:0c:29:a3:4d:9a)
Delete
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.


Status / Dashboard
System Information
Name
pfSense-master.home.arpa
User
admin@172.16.1.1 (Local Database)
System
VMware Virtual Machine
Netgate Device ID: 1366975ce7d281c537c0
BIOS
Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Boot Method: BIOS
Version
2.8.1-RELEASE (amd64)
built on Mon Dec 15 17:31:00 UTC 2025
FreeBSD 15.0-CURRENT
The system is on the latest version.
Version information updated at Tue Apr 21 17:13:42 UTC 2026
CPU Type
AMD Ryzen 7 Microsoft Surface (R) Edition
2 CPUs : 1 package(s) x 2 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto
Inactive
Kernel PTI
Disabled
MDS Mitigation
Inactive
Uptime
02 Hours 00 Minute 58 Seconds
Current date/time
Tue Apr 21 17:43:34 UTC 2026
DNS server(s)
127.0.0.1
::1
10.10.11.2
Last config change
Tue Apr 21 17:37:06 UTC 2026
Netgate Services And Support
Contract type
Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Upgrade Your Support
Community Support Resources
Netgate Global Support FAQ
Official pfSense Training by Netgate
Netgate Professional Services
Visit Netgate.com
If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.
Interfaces
WAN
1000baseT <full-duplex>
10.10.11.168
LAN
1000baseT <full-duplex>
172.16.1.10
SYN
1000baseT <full-duplex>
10.180.0.100

À partir de là, nous pouvons aborder la configuration de la haute disponibilité :

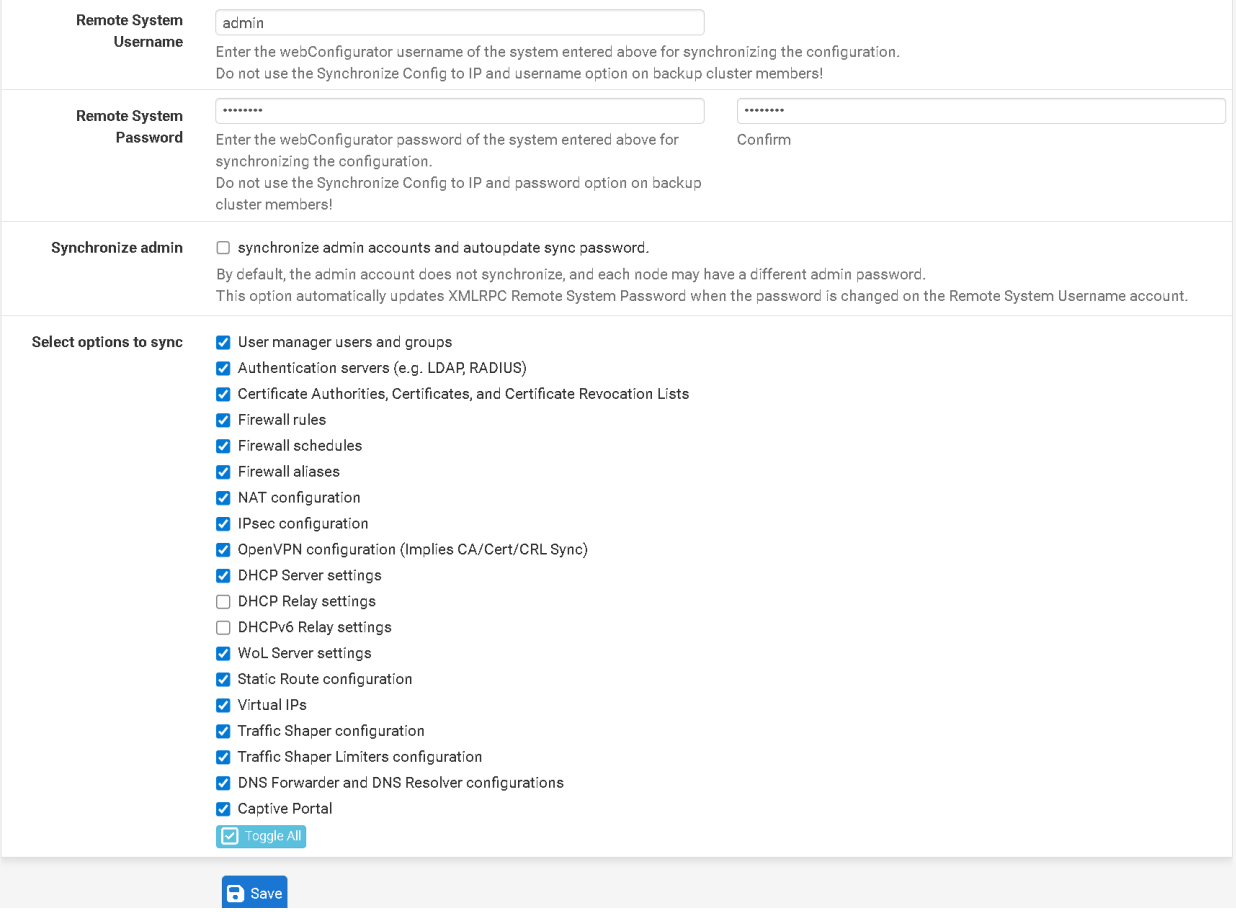


Sur la machine master, on accède à System / High Availability : depuis le master, il faut configurer les deux parties, à savoir pfsync et XMLRPC Sync.

pfsync : synchronisation des connexions en temps réel.

XMLRPC : synchronisation de la configuration.

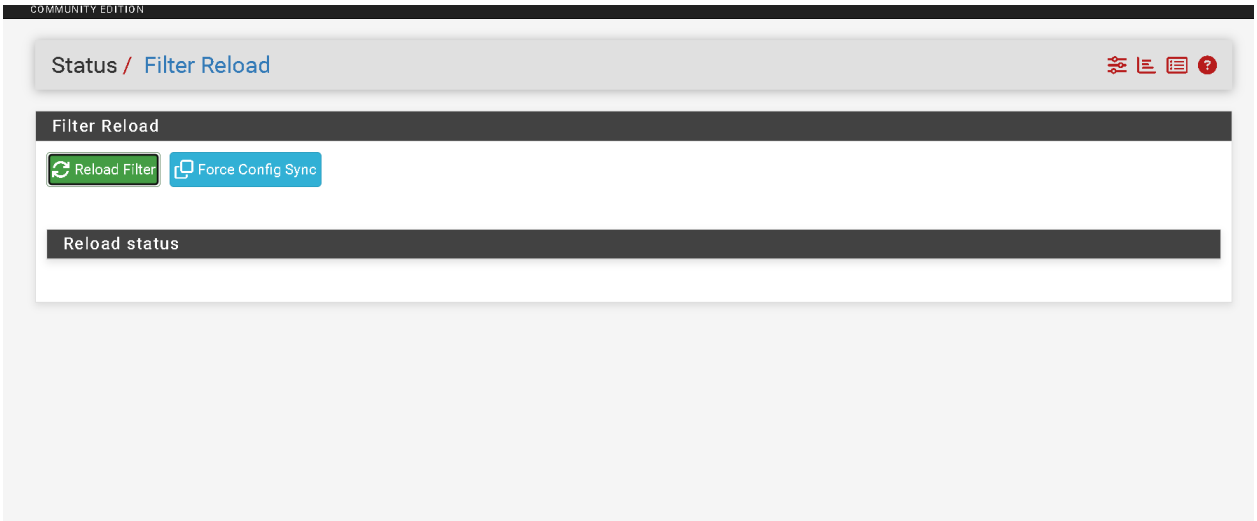
Le pfsync doit être configuré sur les deux pfSense (bidirectionnel), tandis que le XMLRPC ne doit être configuré que sur le Master (unidirectionnel).



Ici, on renseigne les identifiants du backup et on active les paramètres que l'on souhaite synchroniser entre les deux routeurs.

L'étape suivante, obligatoire, consiste à créer une règle sur les deux pfSense, sur l'interface SYNC chargée d'effectuer la synchronisation.

Pour vérifier que tout fonctionne correctement, utiliser l'option « Filter Reload ».



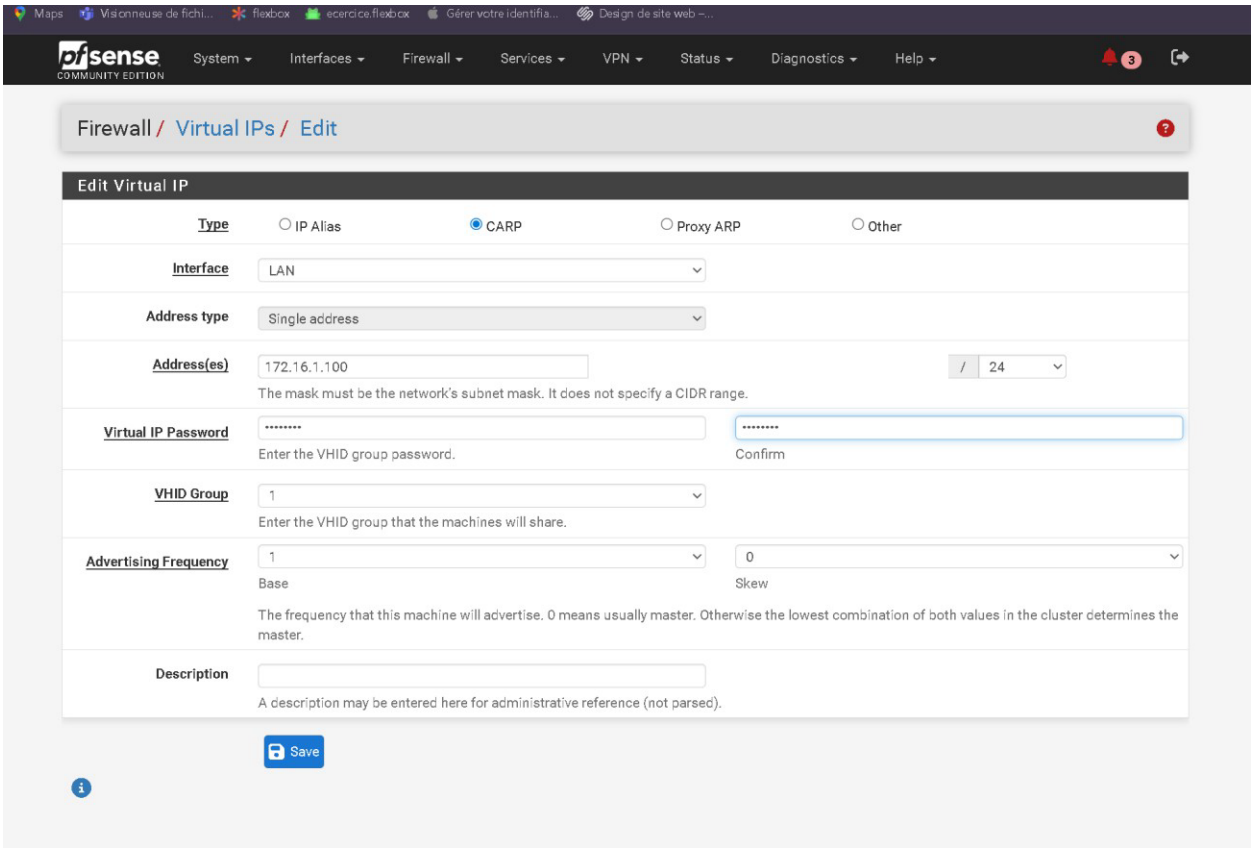
Appuyer sur « Force Config Sync » pour forcer la synchronisation entre les deux routeurs.

Comme on le constate ici, les logs confirment que la synchronisation s'effectue correctement entre les deux pfSense. On peut également effectuer un test en créant un utilisateur sur le master, puis en vérifiant sur le backup si cet utilisateur a bien été créé.

L'étape de synchronisation est terminée. Nous passons maintenant à une autre partie du TP, en lien avec celle que nous venons de réaliser.

Pour simplifier la gestion de la Gateway, nous allons mettre en œuvre une VIP (Virtual IP) via le protocole CARP, afin de créer une carte réseau virtuelle et une adresse IP virtuelle. Cette adresse n'existe pas physiquement, n'est rattachée à aucune machine en particulier et peut basculer entre les deux pfSense.

Les étapes pour mettre en place la VIP (IP virtuelle) :

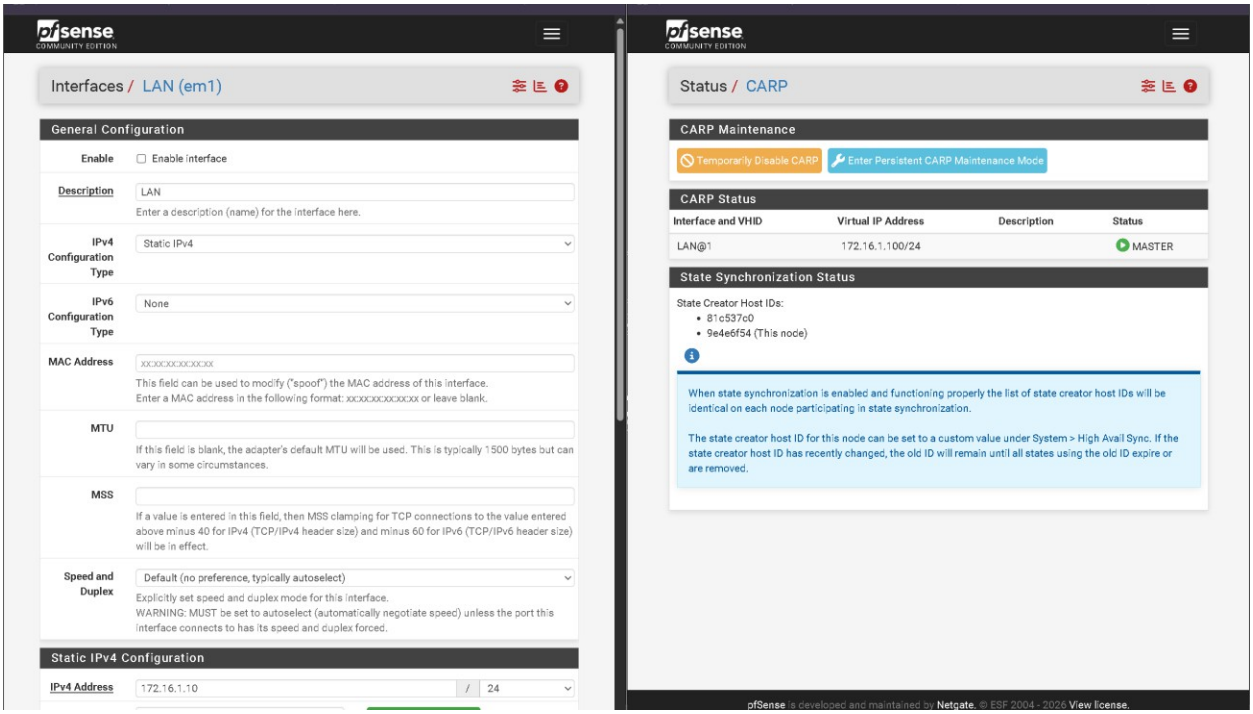


Dès que la configuration est effectuée sur le master, la réplication est automatiquement appliquée sur le backup, ce qui optimise et réduit la charge de travail.

Le mécanisme CARP utilise les paramètres Base et Skew pour déterminer la priorité des nœuds. Le nœud ayant la valeur la plus faible devient actif et envoie les messages de heartbeat.

La configuration a été répliquée sur le backup via le XMLRPC précédemment mis en place.

Ici, on constate que CARP distingue bien le master du backup. Pour tester le basculement, nous allons éteindre le master afin de vérifier si le backup prend effectivement le relais.

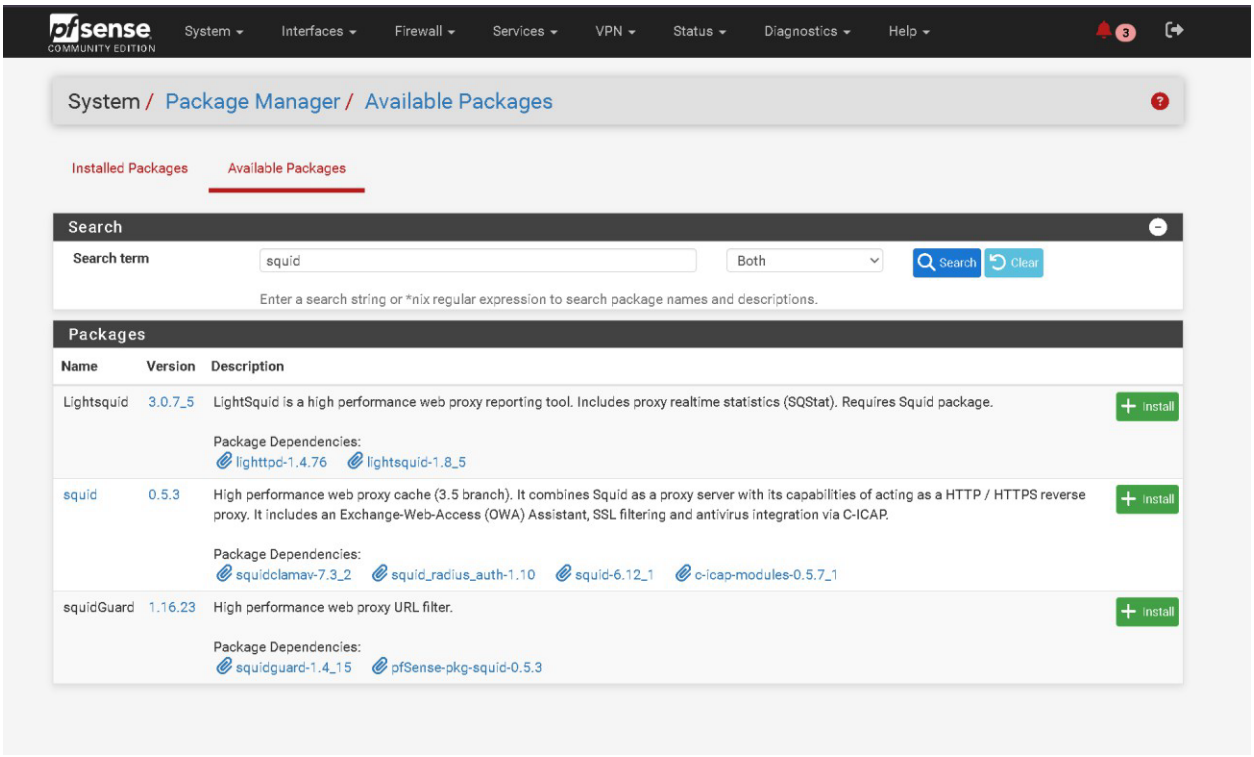


On constate bien que lorsque le master tombe en panne, le backup prend le rôle de master.

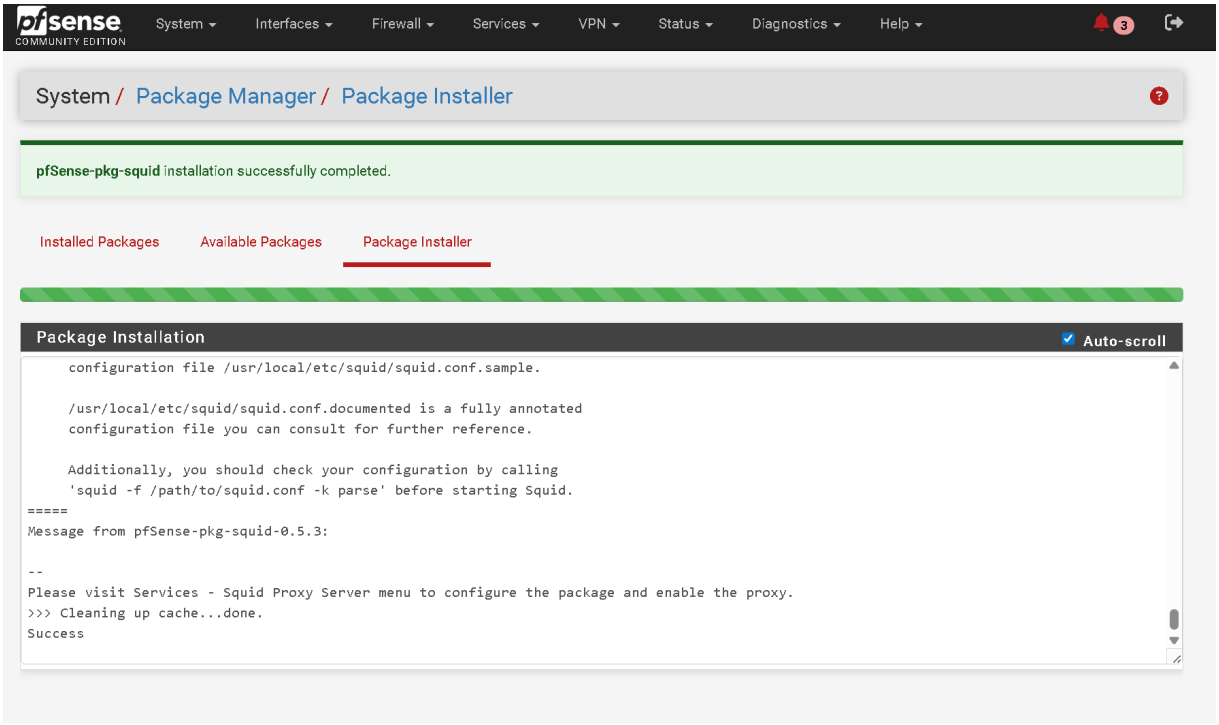
2. Déployer Squid Proxy et l'associer au serveur FreeRADIUS sur pfSense :

Configuration d'un Proxy Squid non transparent sur pfSense : Sans authentification, avec RADIUS et blocage de sites web

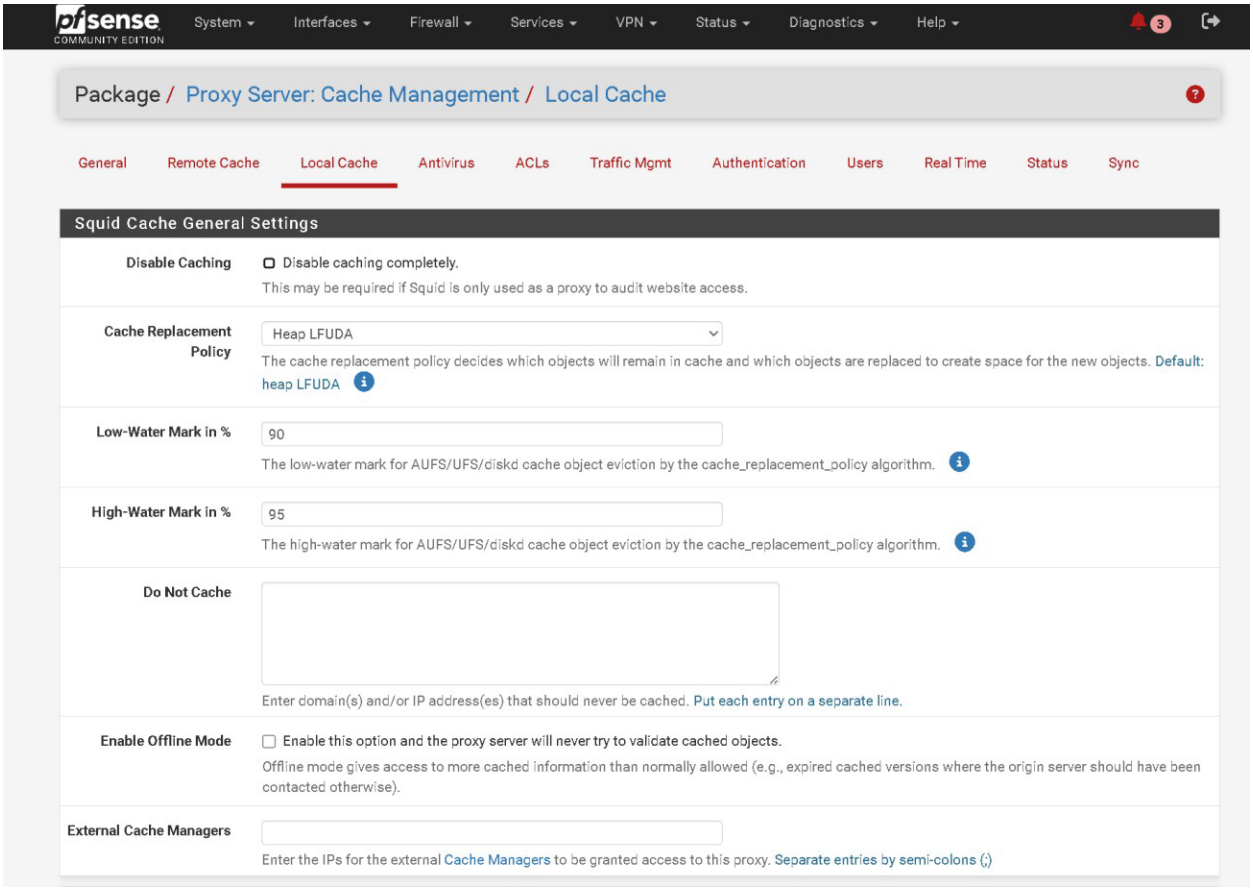
I. **Configuration d'un Proxy Squid non transparent sur pfSense sans authentification, blocage de sites web**
   1. Télécharger Squid
   2. Activer le Cache Local du Proxy Squid
   3. Activer le Proxy Squid
   4. Ajouter les sites web à bloquer
   5. Créer une règle pour permettre aux utilisateurs du réseau LAN d'accéder à Internet via un proxy Squid.
   6. Désactiver le NAT OUTBOUND
   7. configuration manuelle du proxy sur le poste client du réseau LAN
   8. Tester la navigation sur internet
   9. Tester l'accès aux sites web bloqués



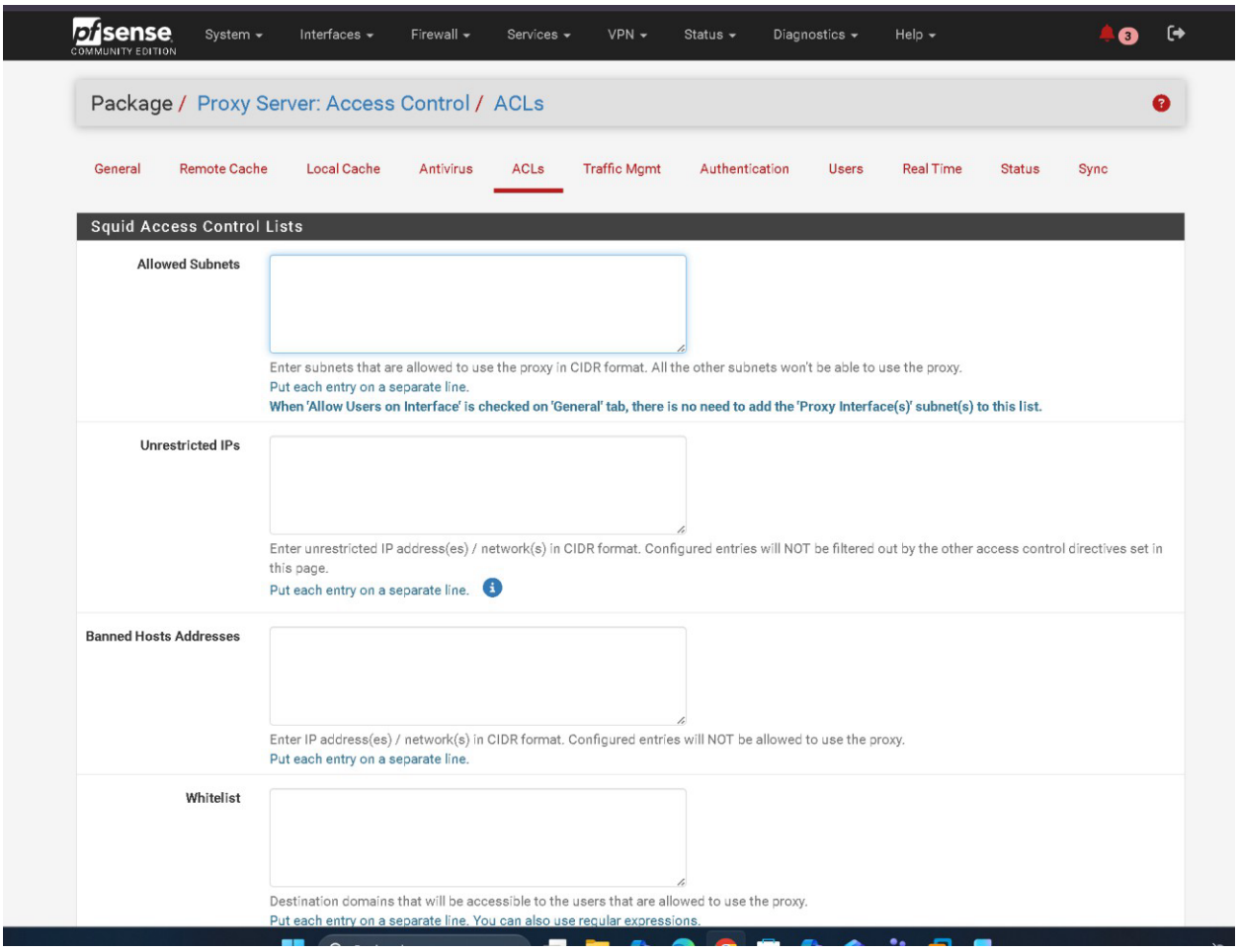
Installation du paquet Squid Proxy sur pfSense.

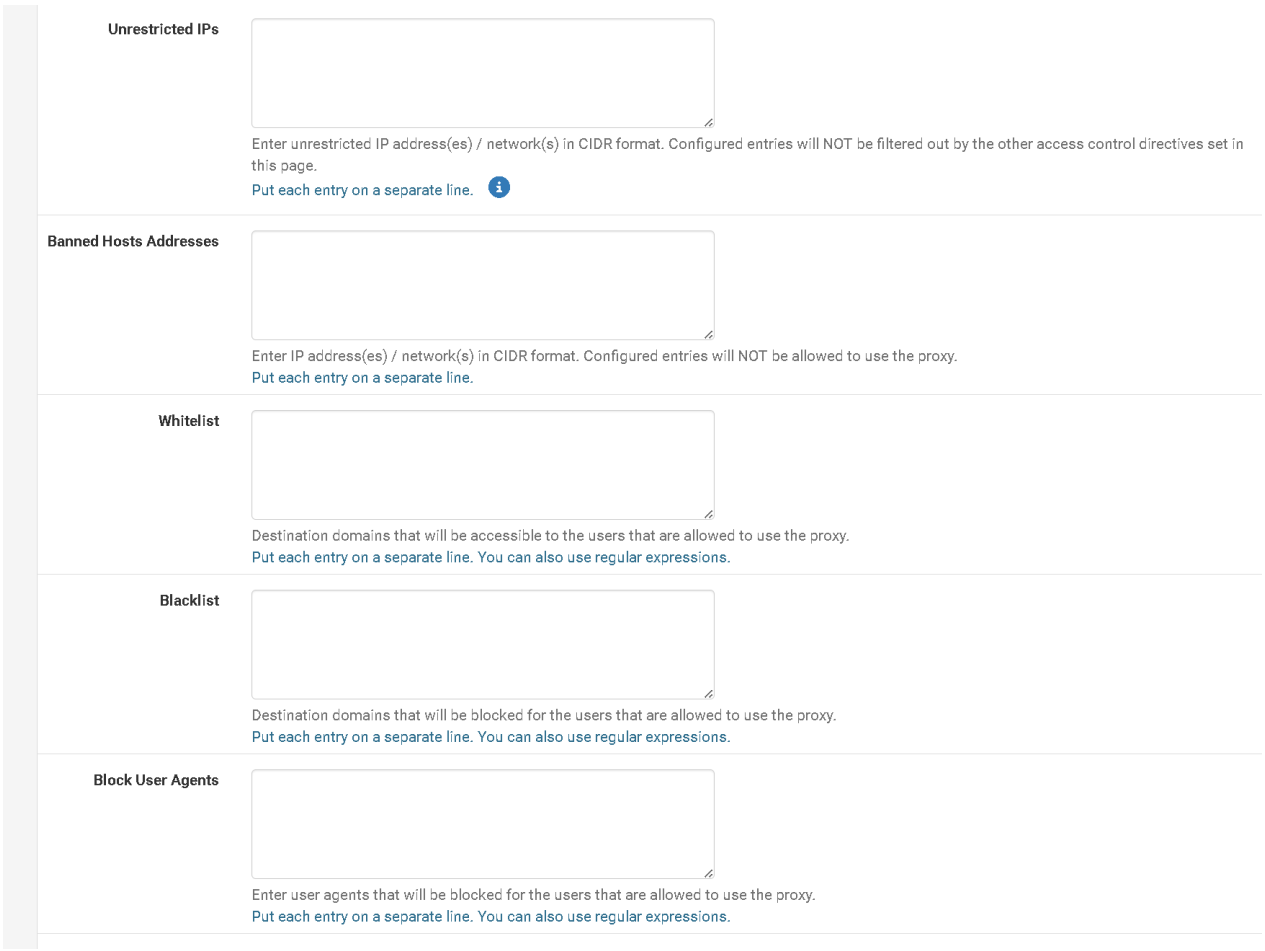


L'installation du paquet est effectuée avec succès.

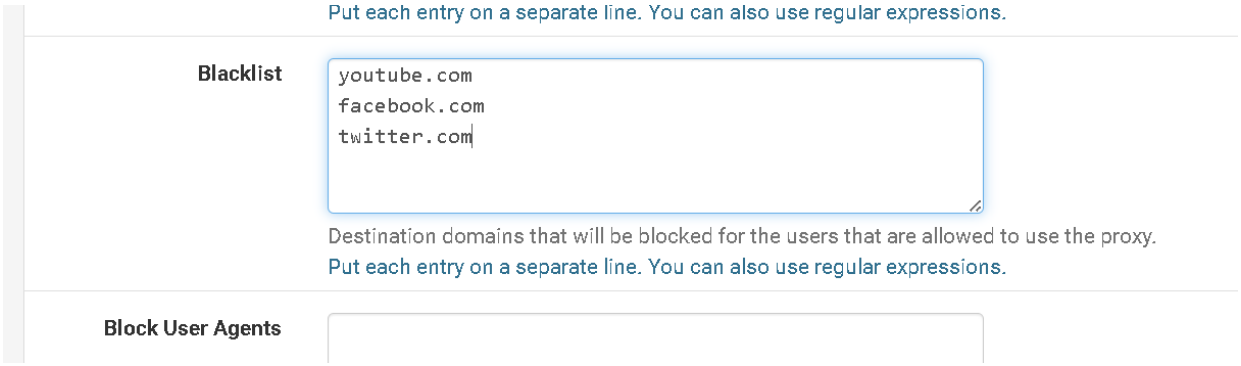


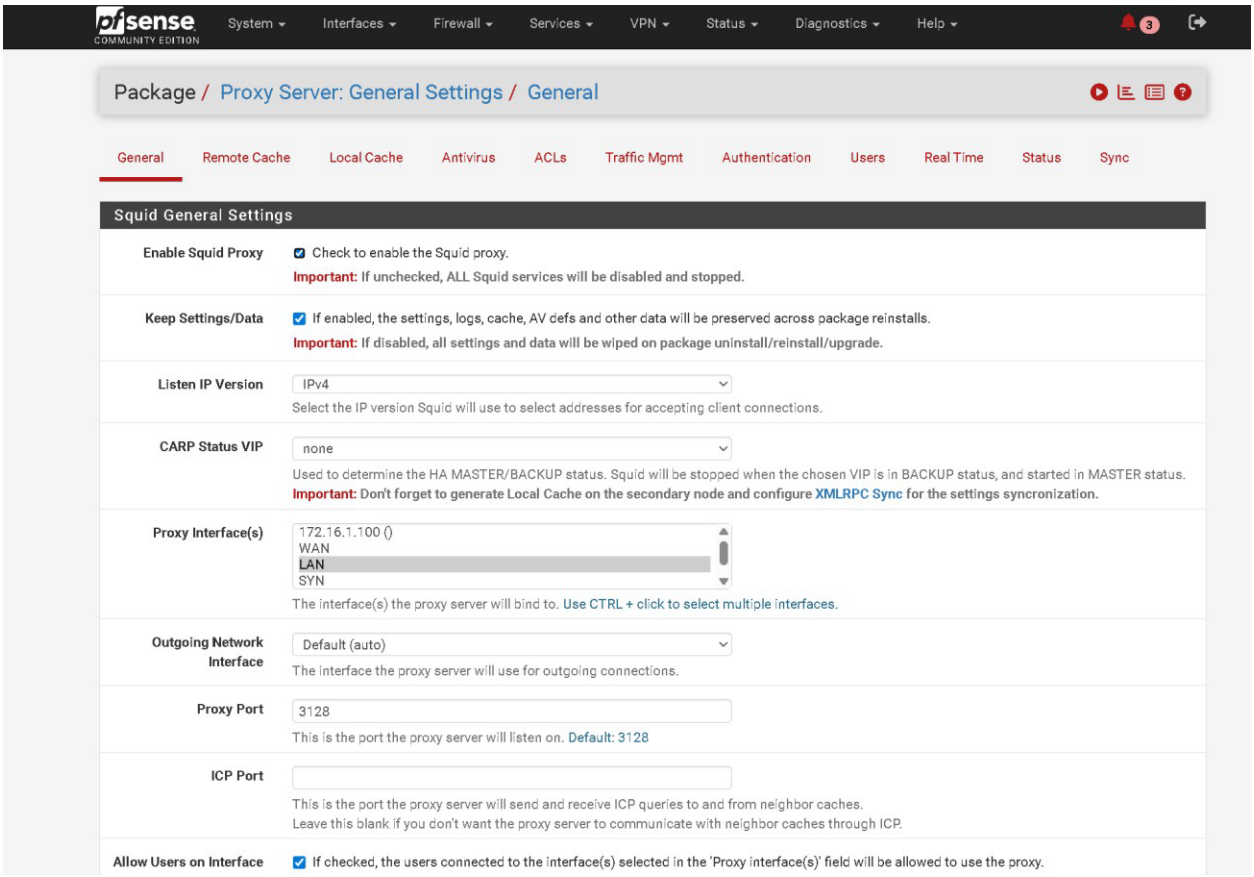
Activation du cache de Squid Proxy.


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
3
Package / Proxy Server: Access Control / ACLs
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
Squid Access Control Lists
Allowed Subnets
Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.
Put each entry on a separate line.
When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.
Unrestricted IPs
Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.
Put each entry on a separate line.
Banned Hosts Addresses
Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.
Put each entry on a separate line.
Whitelist
Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

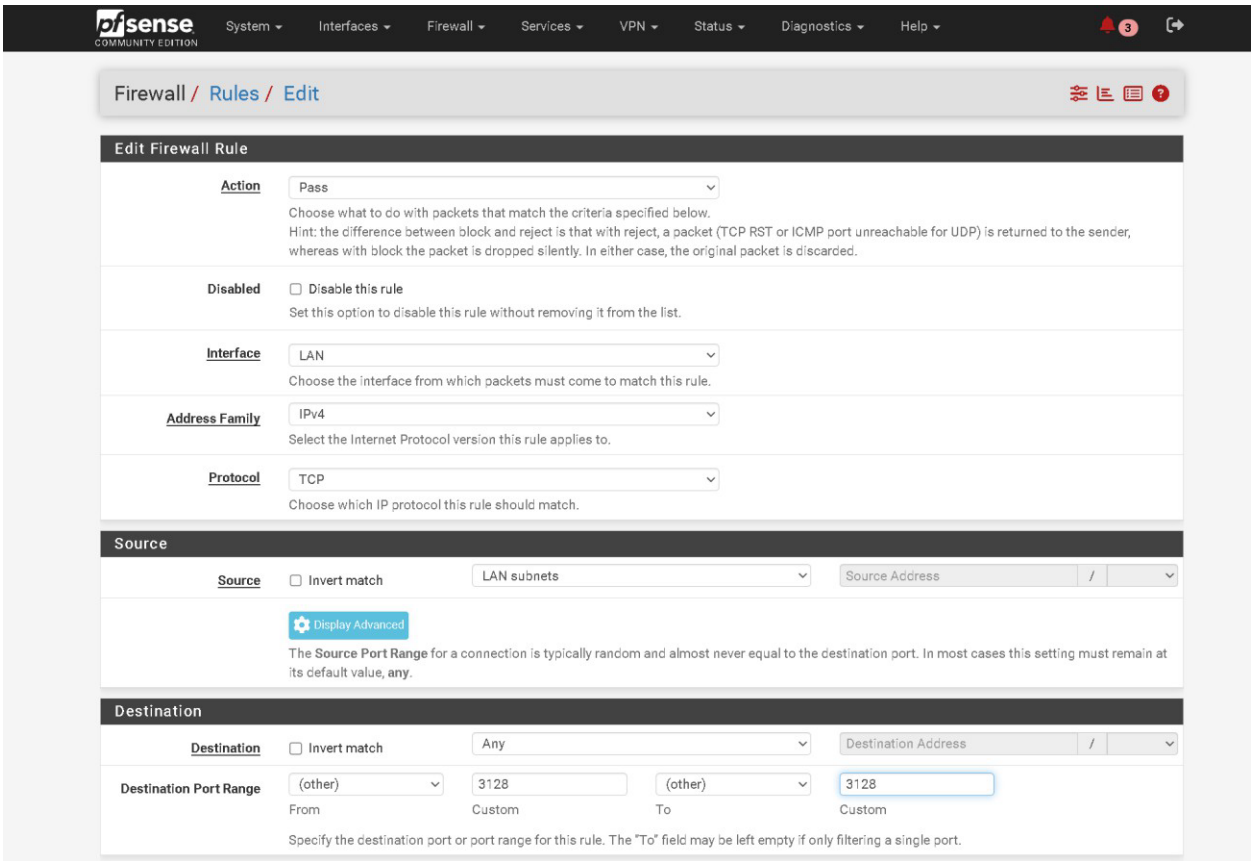


Dans l'onglet « Blacklist », on saisit les sites auxquels les utilisateurs ne doivent pas pouvoir accéder.

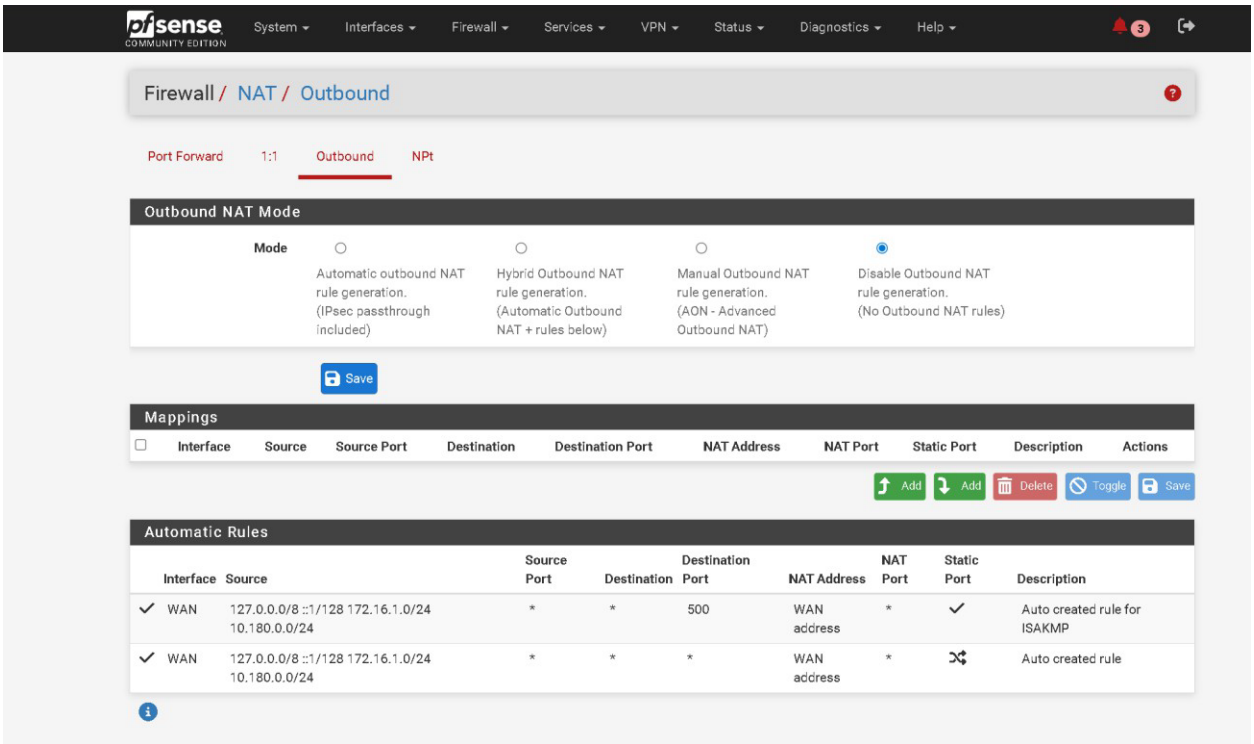




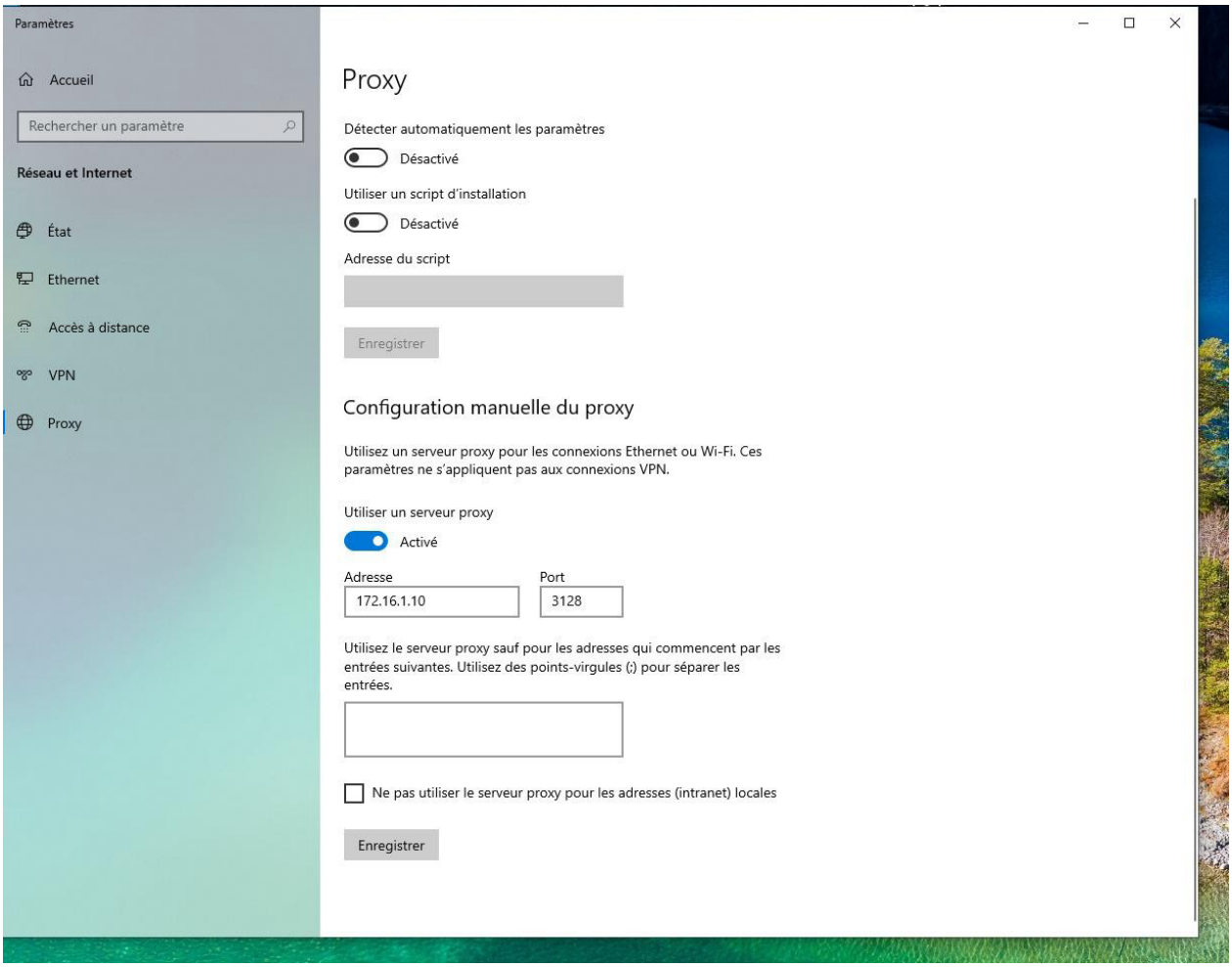
Activation du proxy Squid.



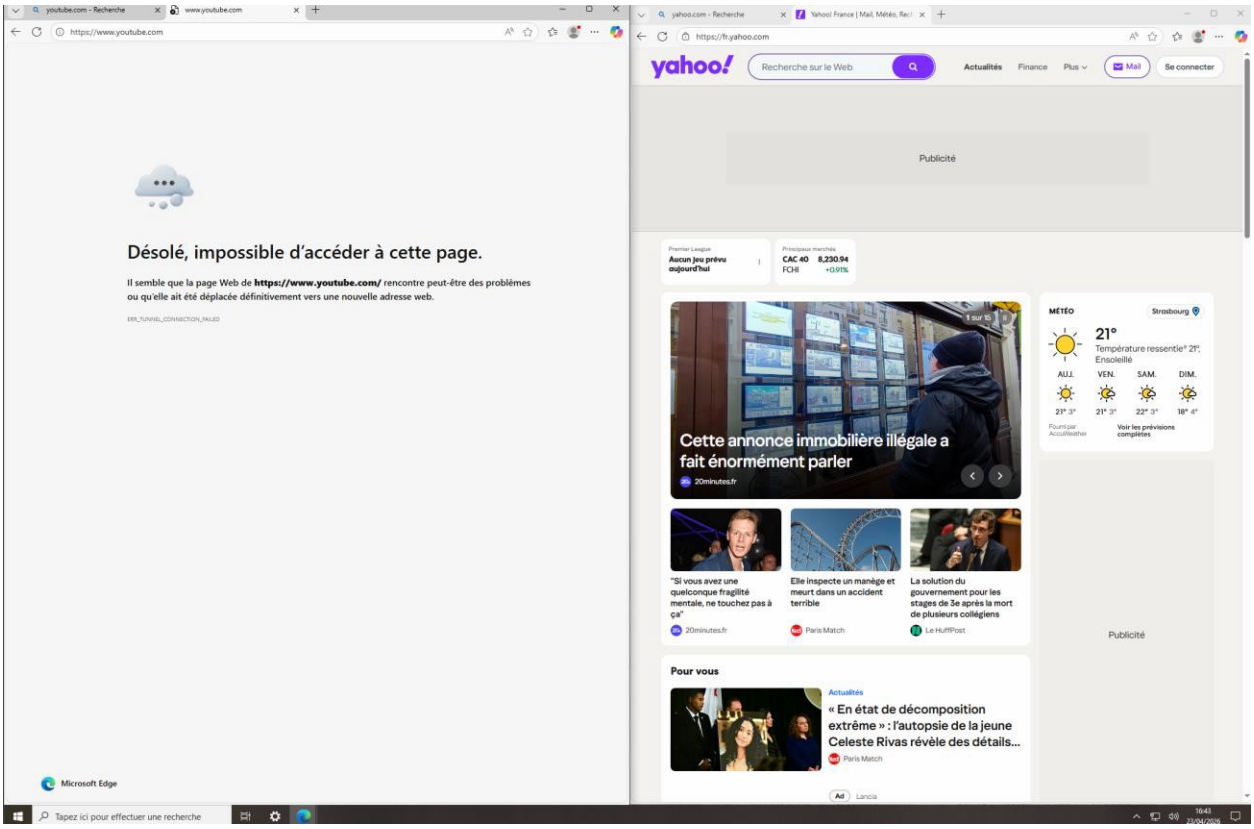
Activation d'une règle permettant aux utilisateurs du réseau LAN d'accéder à Internet via le proxy Squid.



Désactivation du NAT OUTBOUND afin de forcer les utilisateurs à accéder à Internet via le proxy Squid, conformément à la règle définie précédemment.



Configuration manuelle du proxy sur le poste client du réseau LAN.

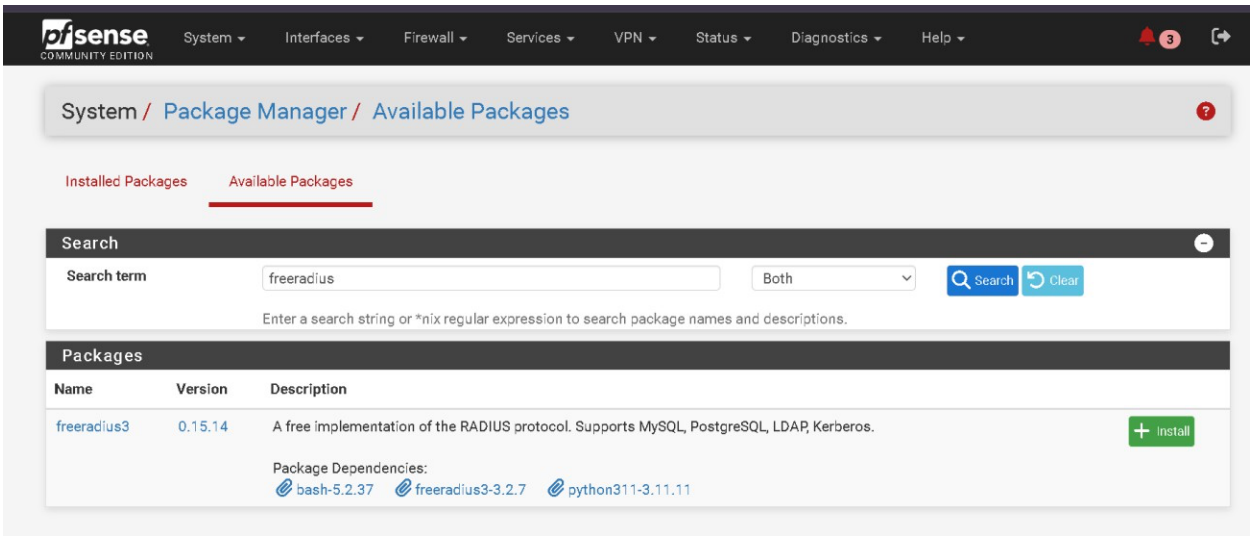


Les services fonctionnent correctement, conformément à ce qui était souhaité.

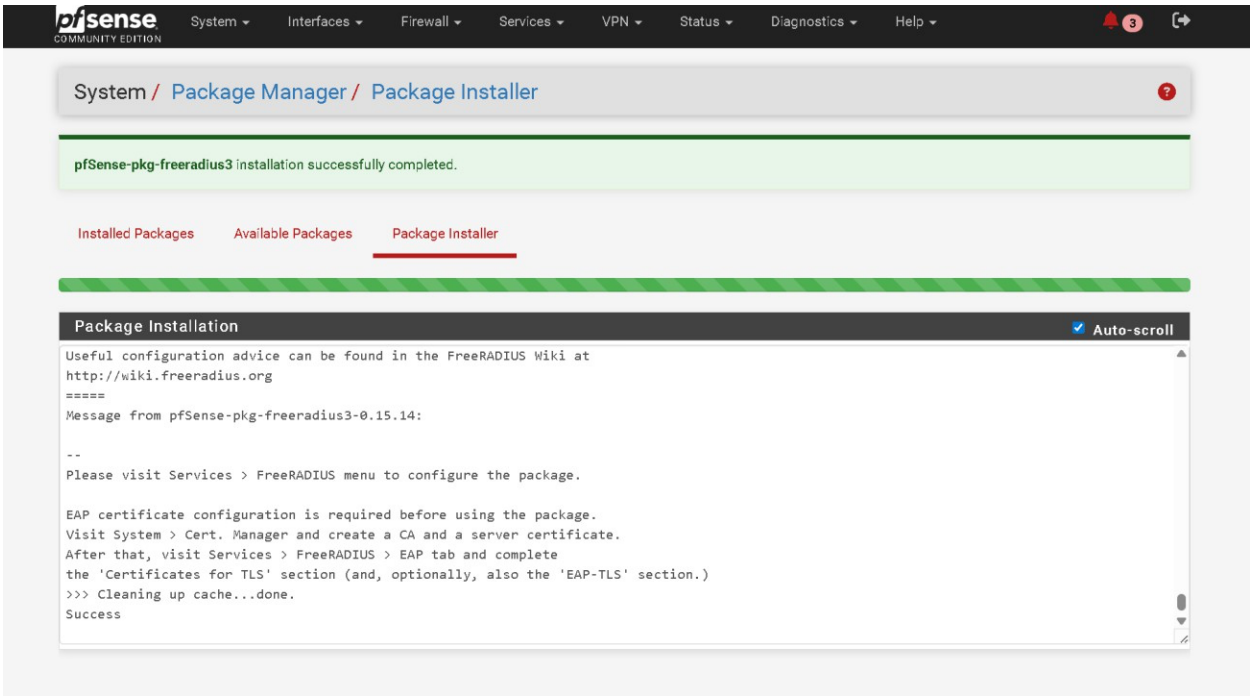
3. Configuration d'un proxy Squid non transparent sur pfSense avec authentification RADIUS

Les étapes indispensables pour associer l'authentification FreeRADIUS au proxy Squid :

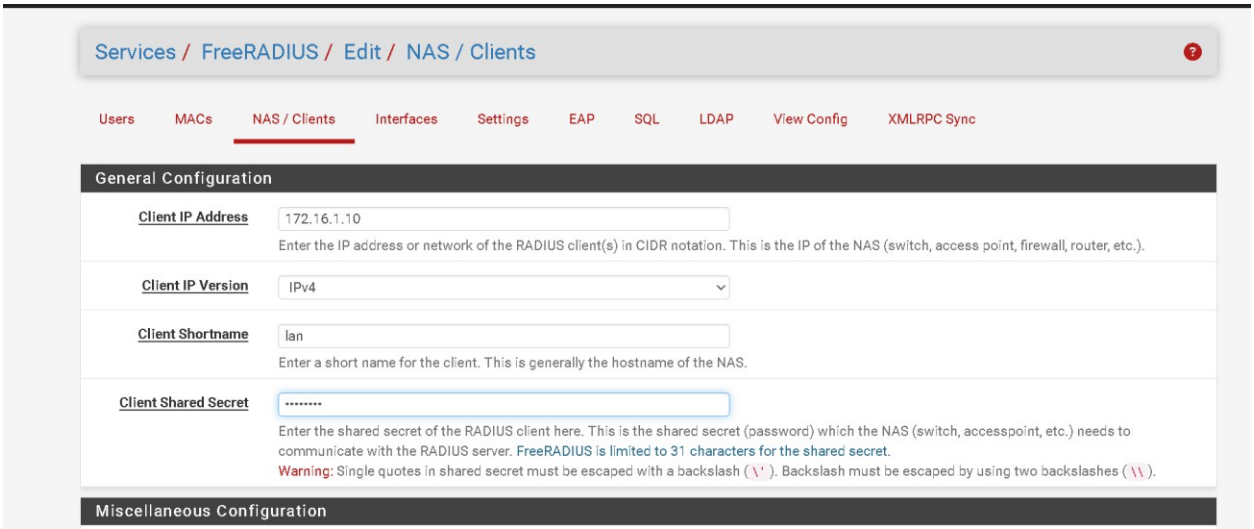
1. **Installer FreeRADIUS 3 ;**
2. **Configurer le NAS/Client dans FreeRADIUS ;**
3. **Configurer les interfaces de FreeRADIUS ;**
4. **Définir FreeRADIUS comme méthode d'authentification sur le proxy ;**
5. **Créer un compte utilisateur sur FreeRADIUS ;**
6. **Ajouter RADIUS comme serveur d'authentification.**



Installation de FreeRADIUS 3.

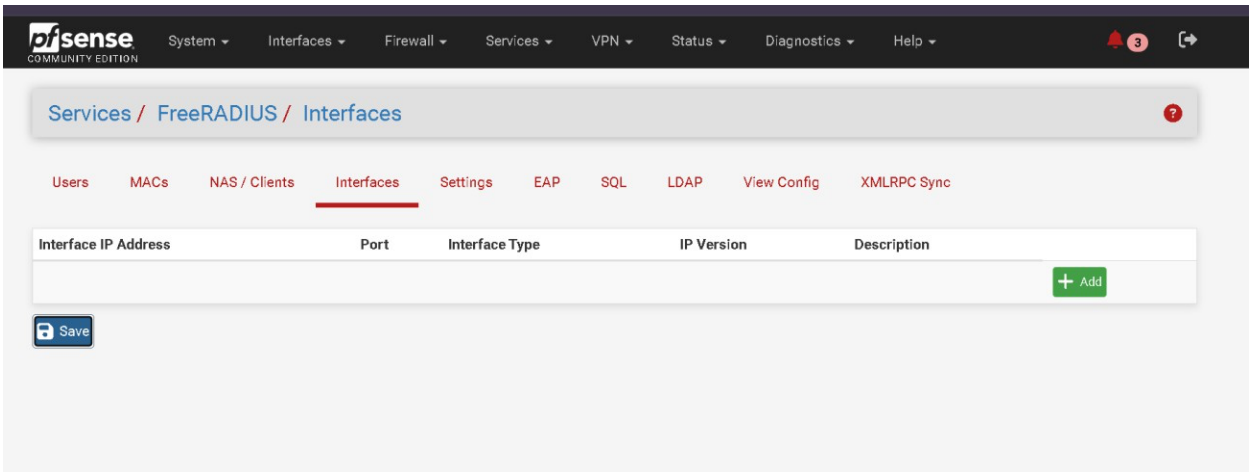


L’installation est terminée avec succès.

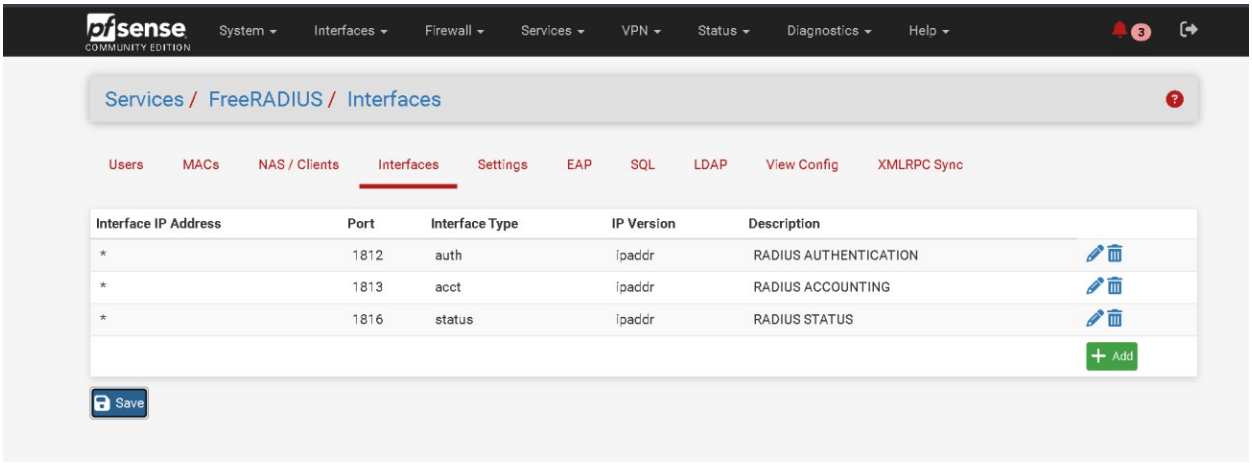


Configuration du NAS/Client dans FreeRADIUS.

NAS/Client : il s’agit d’un service qui permet au proxy d’envoyer la demande ou la requête d’authentification au serveur RADIUS.



Ici, nous configurons les interfaces du serveur RADIUS, c'est-à-dire les interfaces sur lesquelles le serveur RADIUS va écouter.



Pourquoi 3 entrées dans FreeRADIUS ?

FreeRADIUS sépare les fonctions en 3 types de trafic :

1. Authentication (auth) — Port 1812

➡️ C'est le plus important.

– Sert à vérifier les identifiants (login / mot de passe).

Exemple :

- un utilisateur se connecte au Wi-Fi ;
- Le NAS (pfSense, switch, AP, etc.) envoie une requête à FreeRADIUS ;
- FreeRADIUS répond : ACCEPT ou REJECT.

---

2. Accounting (acct) — Port 1813

➡️ Sert à enregistrer l'activité.

– Il enregistre :

- l'heure de connexion ;
- la durée de la session ;
- le volume de données.

Exemple :

- utile pour le portail captif, la facturation et les journaux de sécurité.

---

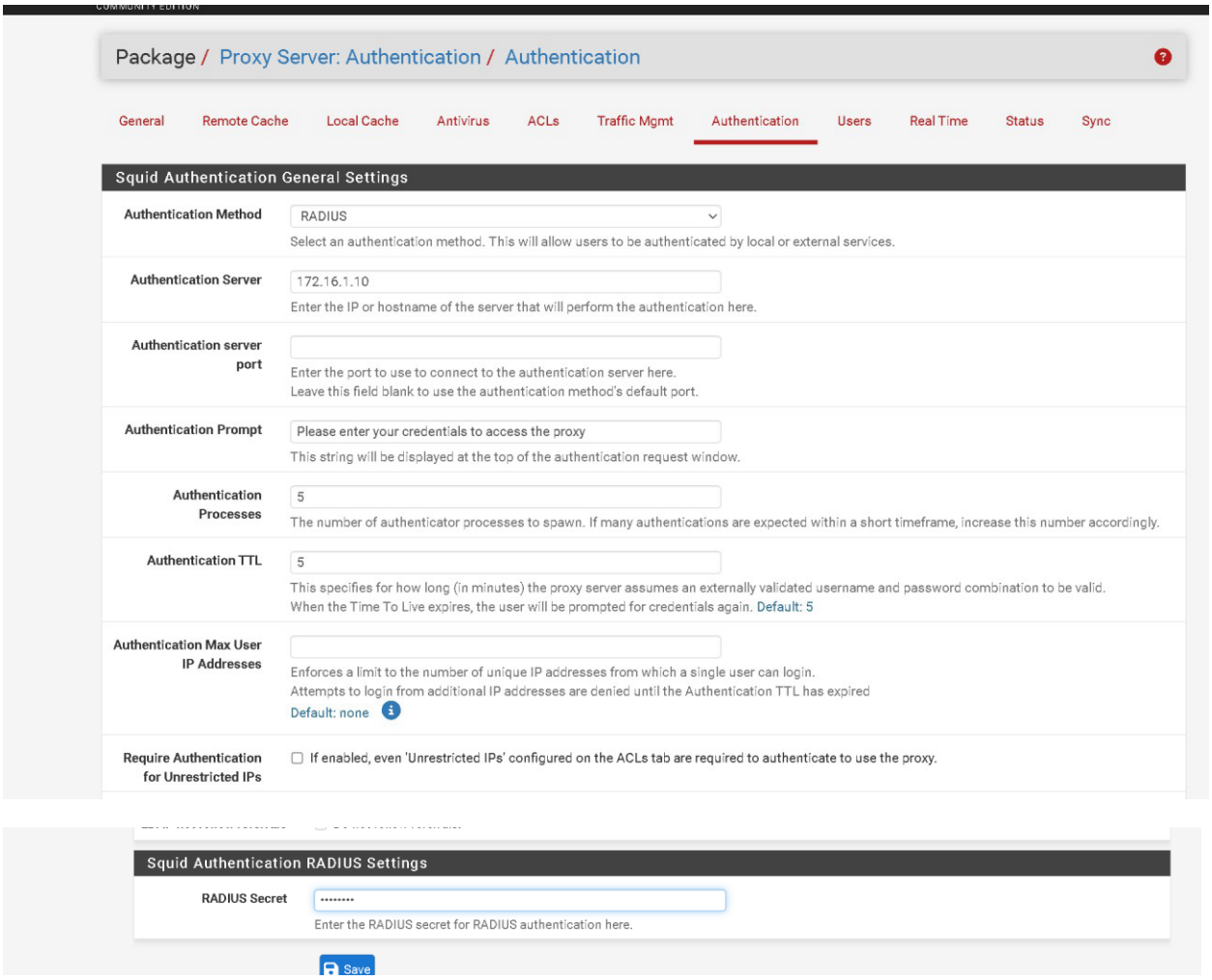
3. Status — Port 1816

⬛ Sert à vérifier si le serveur RADIUS fonctionne.

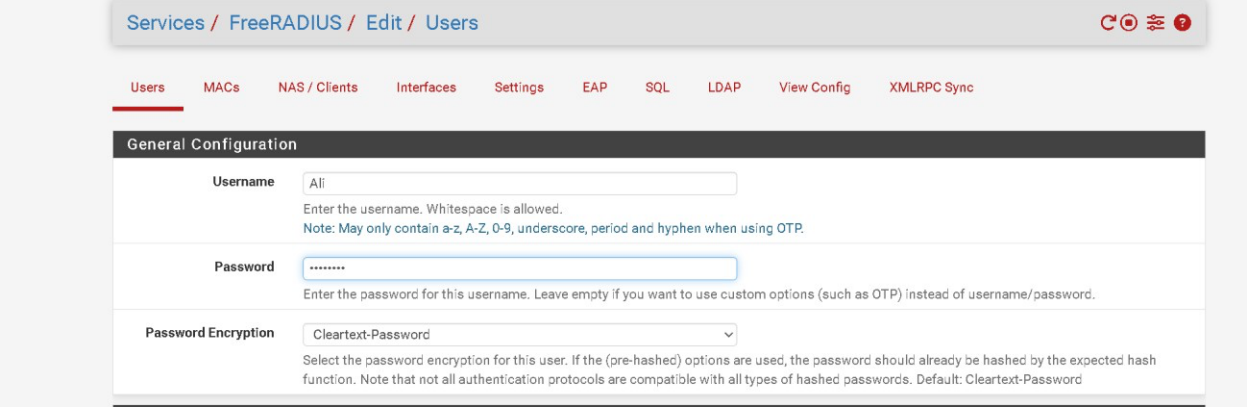
– C'est en quelque sorte un ping RADIUS.

- le NAS peut tester si FreeRADIUS est disponible ;

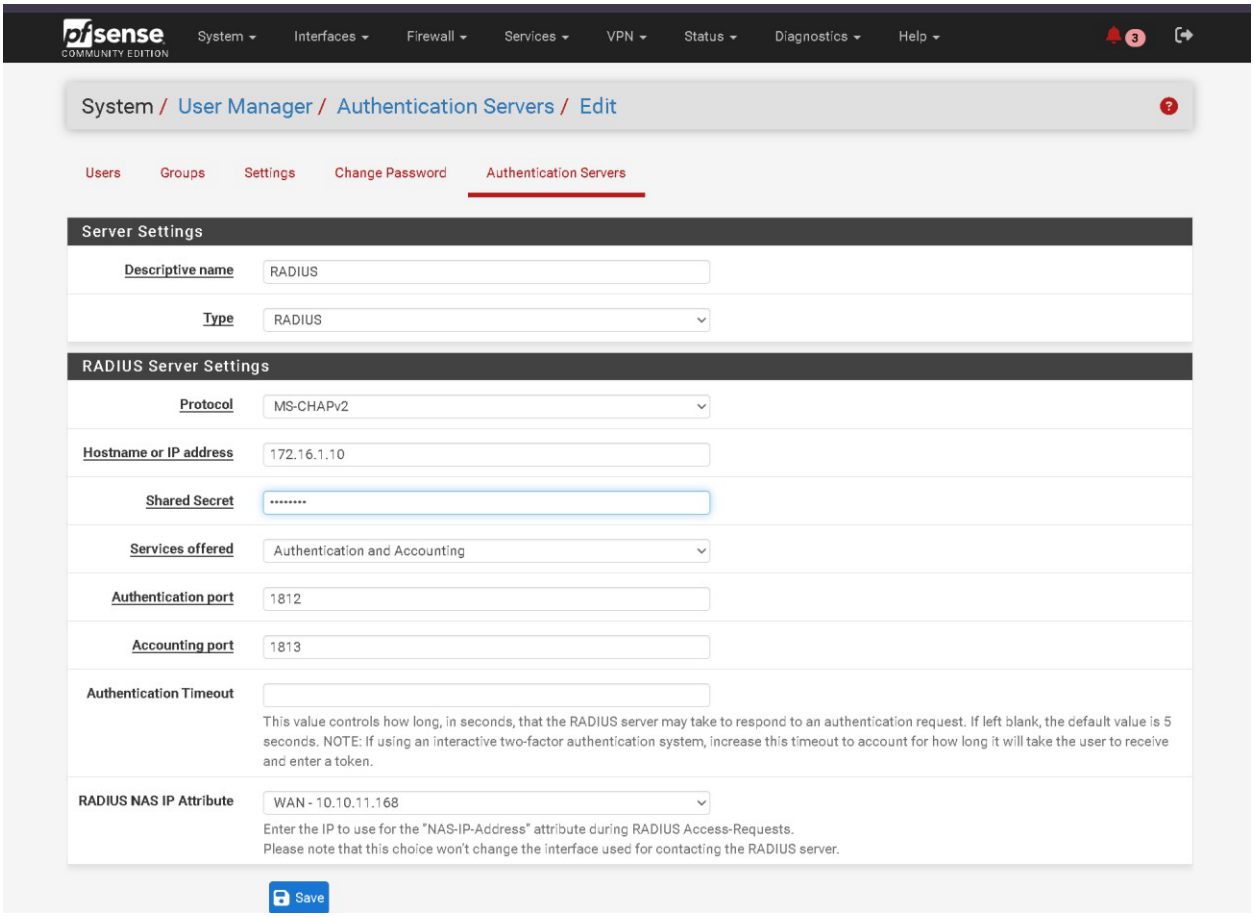
- **utilisé pour le monitoring ou la haute disponibilité (HA).**



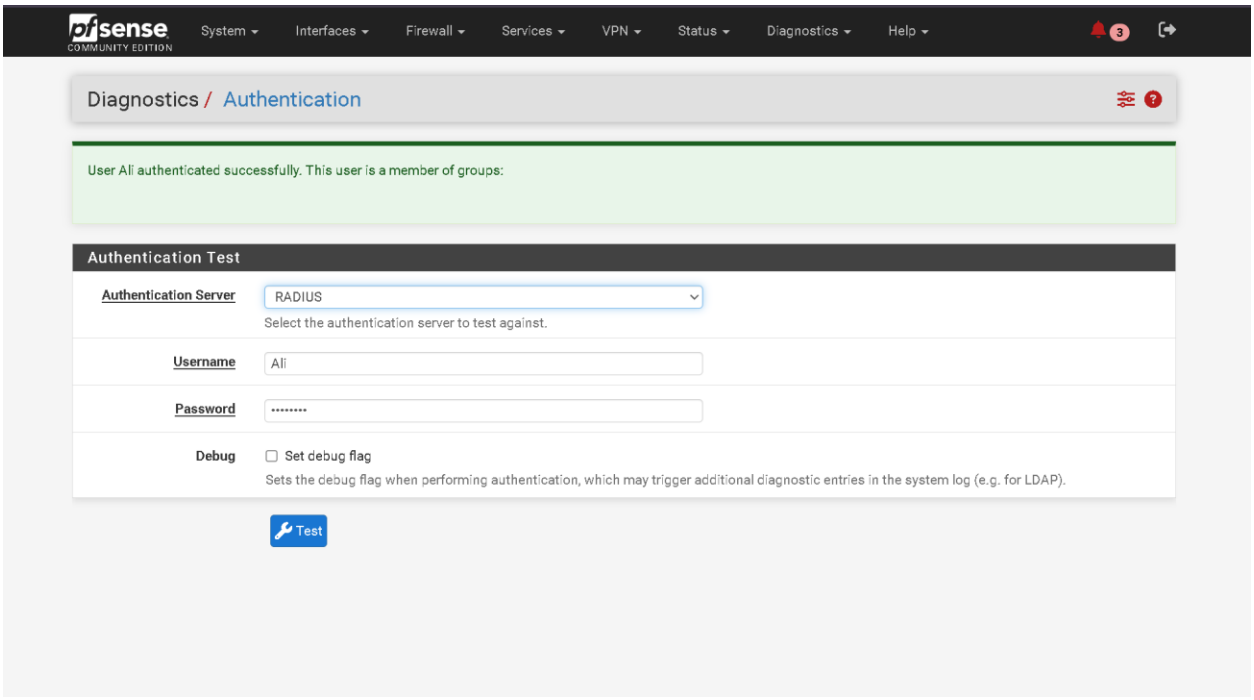
Définir FreeRADIUS comme méthode d'authentification sur le proxy.



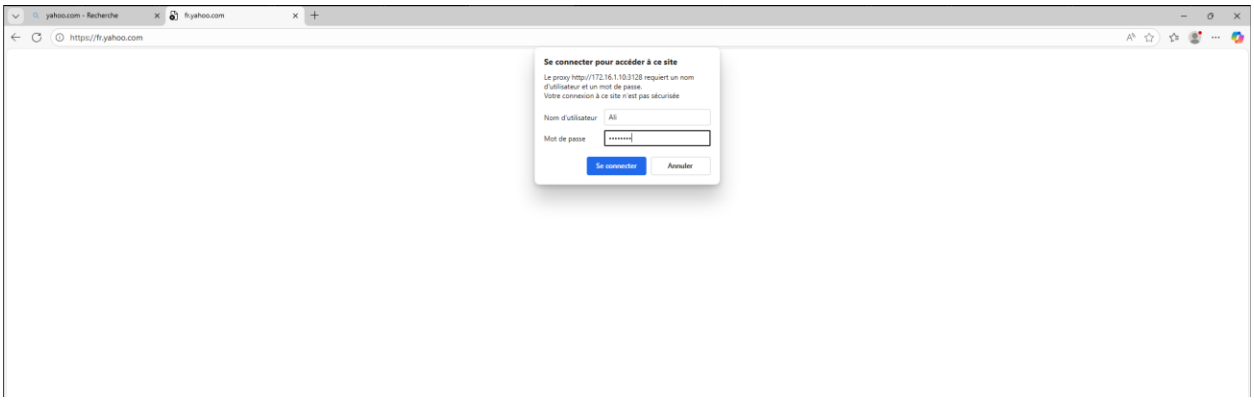
Création d'un compte utilisateur dans FreeRADIUS.



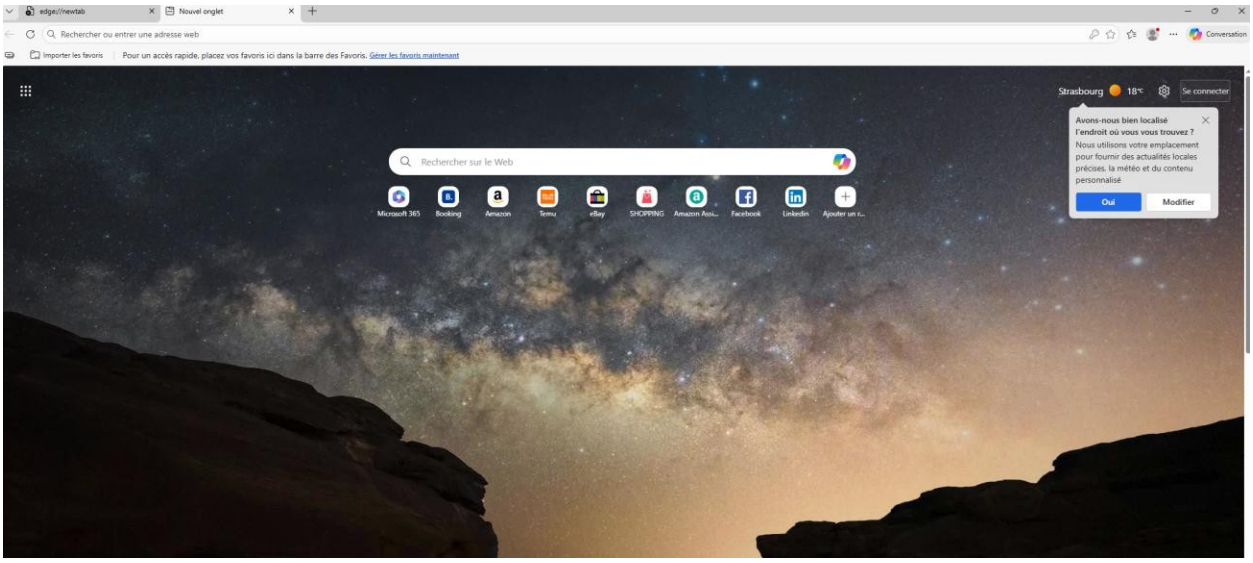
Ajout de RADIUS comme serveur d'authentification.



Test de l'authentification sur le serveur RADIUS.



Test sur la machine cliente : tout fonctionne correctement.



Après avoir saisi correctement les identifiants, l'accès à Internet est autorisé.

FIN DU PROJET

- **Amir Tajik**