

Installation radius :

Je fais d'abord un routeur pfsense auquel j'y connecte une machine ubuntu, c'est sur cette machine que je vais installer radius.

Tout d'abord je commence par faire ces commandes, pour mettre a jour les paquets et ensuite installer freeradius :

```
user@user-None:~$ sudo apt-get update
```

```
user@user-None:~$ sudo apt-get install freeradius
```

Ensuite je vais avoir besoin d'ajouter des clients FreeRadius aux clients.conf, je fais donc cette commande pour le localiser

```
user@user-None:~$ sudo find /etc -name "clients.conf"  
/etc/freeradius/3.0/clients.conf
```

Ensuite une fois localisé, je le modifie avec cette commande

```
user@user-None:~$ sudo nano /etc/freeradius/3.0/clients.conf
```

Ensuite une fois dans le document.conf j'ajoute ces lignes et je sauvegarde et valide

```
client PFSENSE {  
    ipaddr = 192.168.1.1  
    secret = Root123  
}
```

Ensuite je vais devoir modifier le fichier de configuration des utilisateurs Freeradius, je fais donc cette commande pour le localiser x

```
user@user-None:~$ sudo find /etc -name "users"  
/etc/freeradius/3.0/users
```

Ensuite je fais cette commande pour rentrer dedans et le modifier

```
user@user-None:~$ sudo nano /etc/freeradius/3.0/users
```

Une fois dans le fichier users, j'ajoute ces lignes a la fin du fichier

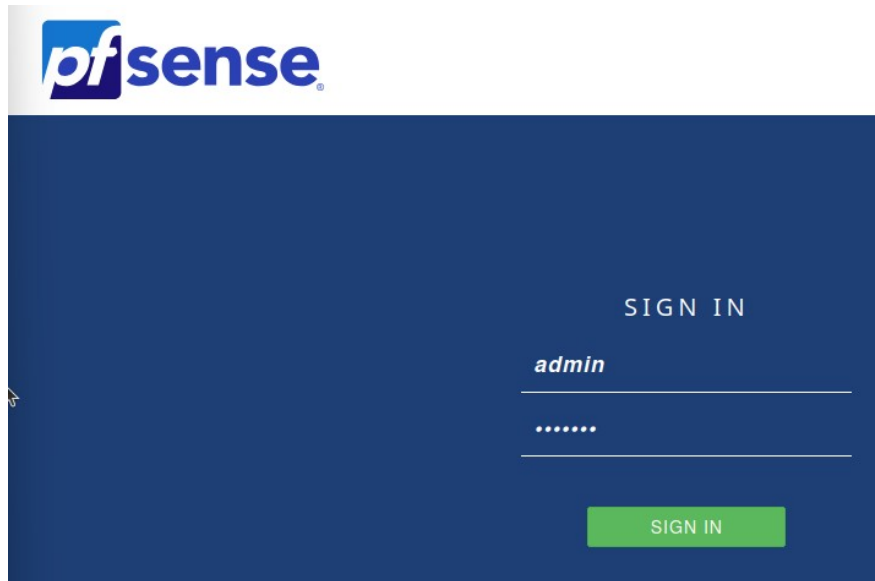
```
Admin Cleartext-password := "Root123"  
    Class = "pfsense-admin"
```

Ensuite je valide mes paramètres et restart mon service avec ces commandes

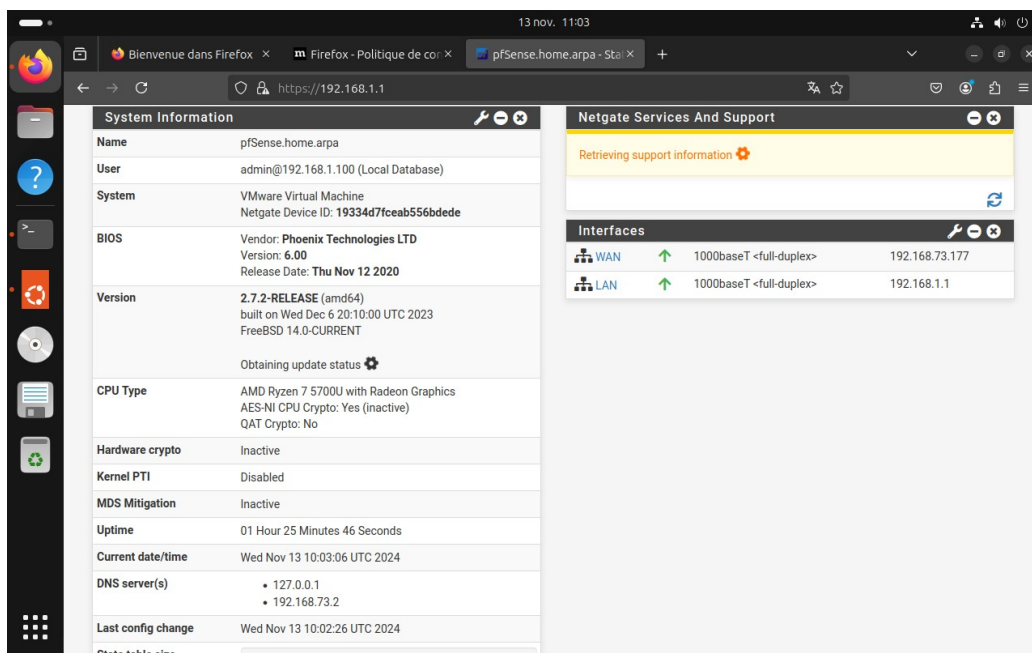
```
user@user-None:~$ sudo freeradius -CX
```

```
user@user-None:~$ sudo service freeradius restart
```

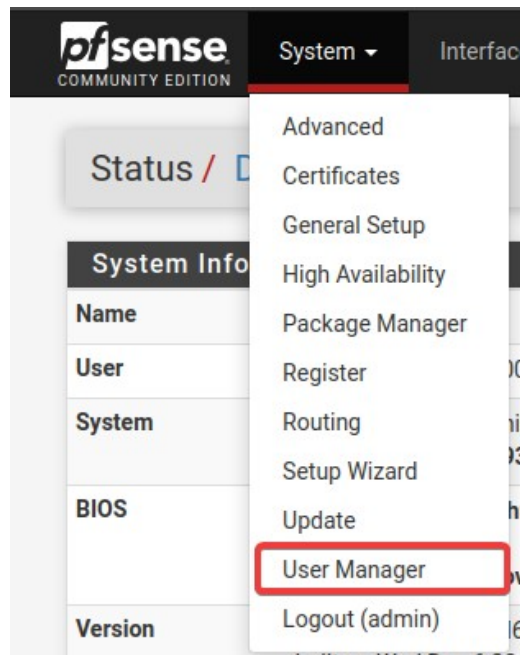
Ensuite nous allons passer à la configuration sous l'interface web de pfsense, je rentre donc l'IP de mon PFSense sur un navigateur et me connecte



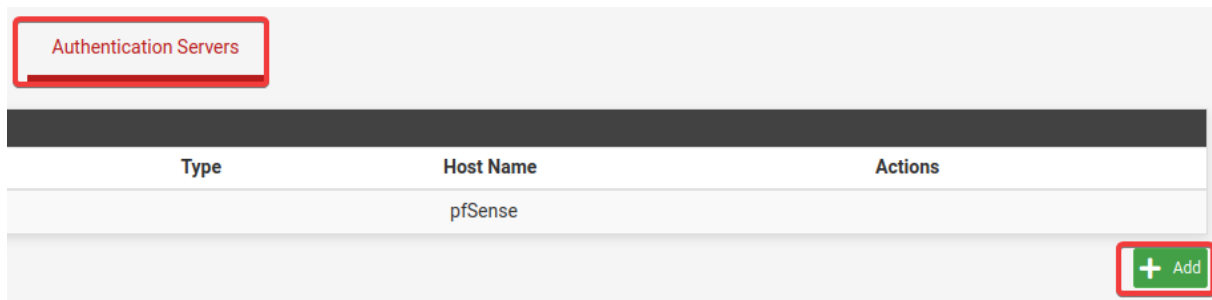
Je configure ensuite mon pfsense en laissant les paramètres de base et en laissant l'IP 192.168.1.1 en IP pour mon pfsense jusqu'à arriver sur cette page



Ensuite je me rend ici dans system et clique sur « user manager »



Ensuite je me rend dans « authentication servers » et clique sur « Add »

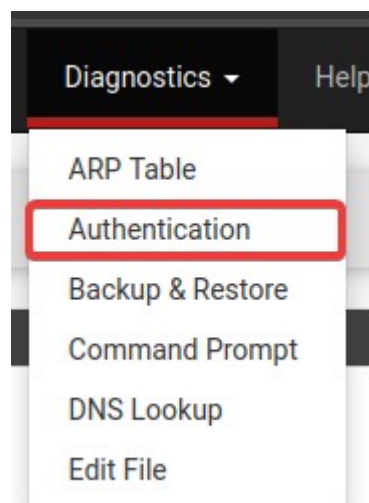


Ensuite pour les paramètres je sélectionne ces paramètres ci

Server Settings	
Descriptive name	RADIUS
Type	RADIUS

RADIUS Server Settings	
Protocol	MS-CHAPv1
Hostname or IP address	192.168.1.100
Shared Secret	*****
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	5
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value of 30 seconds will be used. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take to enter a token.	
RADIUS NAS IP Attribute	WAN - 192.168.73.177
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.	

Ensuite je vais tester l'authentification FreeRadius, je me rend dans diagnostics puis « authentication »



Et ensuite le test fonctionne bien

User Admin authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server RADIUS
Select the authentication server to test against.

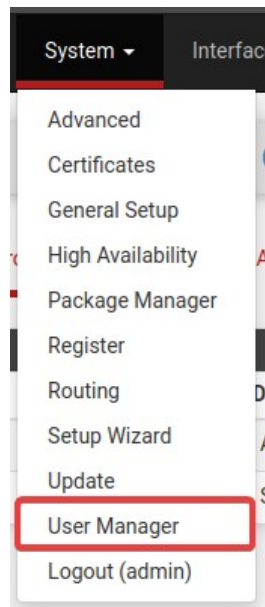
Username Admin

Password *****

Debug ☐ Set debug flag
Sets the debug flag when performing authentication, which may trigger additional logging.

[Test](#)

Ensuite une fois ceci fait, on va autoriser sur PFSense le groupe FreeRadius



Ensuite je vais dans « groups » et je clique sur « Add »

System / User Manager / Groups

Users **Groups** Settings Authentication Servers

Group name	Description	Member Count	Actions
all	All Users	1	Edit Delete
admins	System Administrators	1	Edit Delete

[+ Add](#)

Je met ces paramètres ci

Group Properties

Group name

pfsense-admin

Scope

Remote

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to

Description

Group description, for administrative information only

Group membership

admin

Not members

Members

>> Move to "Members"

<< Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Save

Ensuite au niveau des privilèges je clique sur « Add »

Assigned Privileges

Name	Description	Action

+ Add

Ici je sélectionne WebCfg – all pages et je sauvegarde ces paramètres

Group Privileges

Group

pfsense-admin

Assigned privileges

User - System: Copy files to home directory (chrooted scp)

User - System: Shell account access

User - System: SSH tunneling

User - VPN: IPsec xauth Dialin

User - VPN: L2TP Dialin

User - VPN: PPPoE Dialin

WebCfg - AJAX: Get Queue Stats

WebCfg - AJAX: Get Service Providers

WebCfg - AJAX: Get Stats

WebCfg - All pages

WebCfg - Crash reporter

WebCfg - Dashboard (all)

WebCfg - Dashboard widgets (direct access).

WebCfg - Diagnostics: ARP Table

WebCfg - Diagnostics: Authentication

WebCfg - Diagnostics: Backup & Restore

WebCfg - Diagnostics: Command

WebCfg - Diagnostics: Configuration History

WebCfg - Diagnostics: CPU Utilization

WebCfg - Diagnostics: DNS Lookup

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

Show only the choices containing this term

Et ensuite j'active ces paramètres ici de manière a configurer le mot de passe pfsense avec la base de données RADIUS.

Settings

Session timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server

RADIUS

Password Hash

Algorithm

bcrypt – Blowfish-based crypt

Selects which algorithm the firewall will use when creating hashes for local user passwords.

The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compliance purposes.

Shell Authentication

☐ Use Authentication Server for Shell Authentication

If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used.

To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first.

To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

Save

Save & Test

La configuration du pfsense est donc terminée.

Notre serveur RADIUS est donc maintenant fonctionnel

