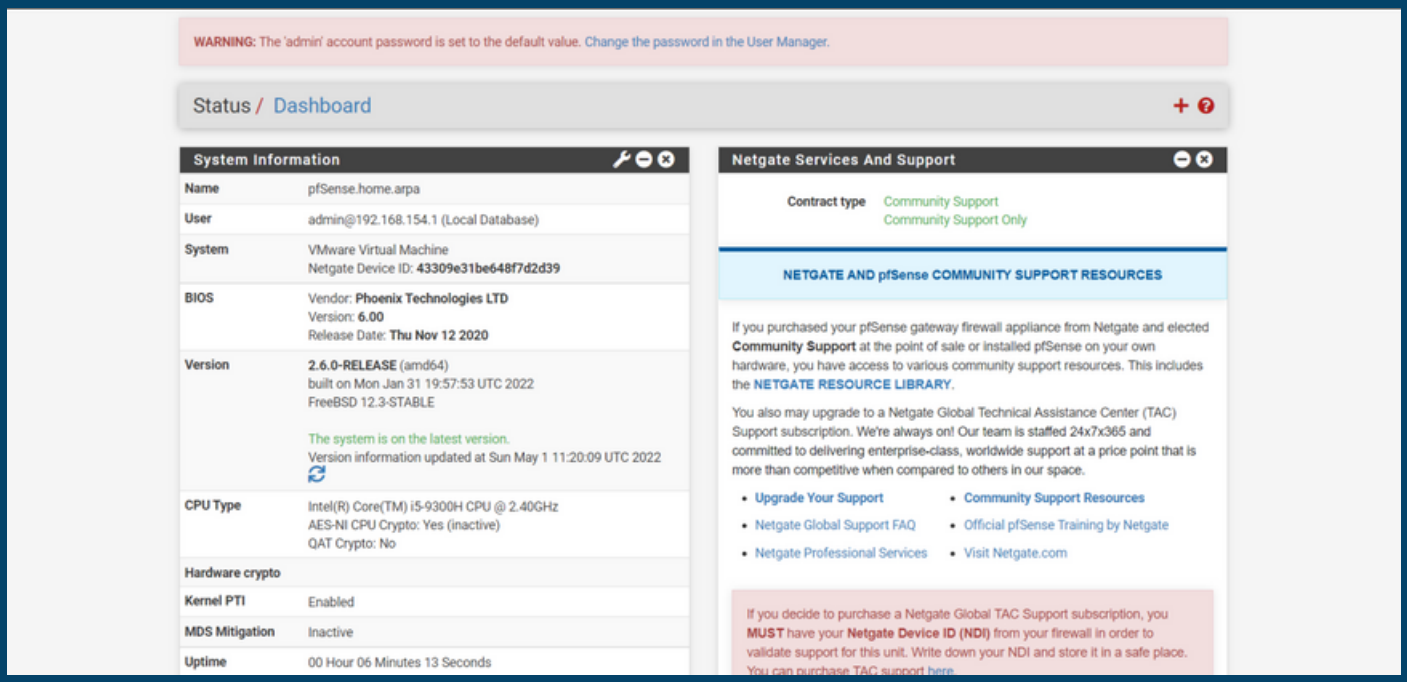
EXPLOITATION PROJET

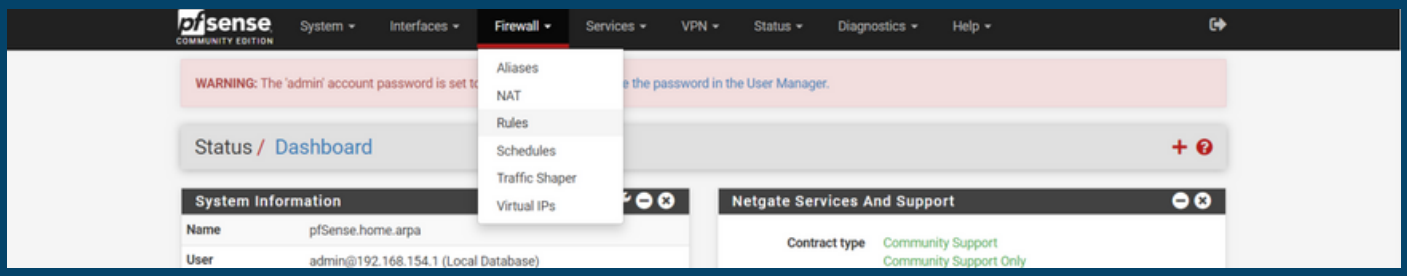
MISE EN APPLICATION

UTILISATION PFSENSE

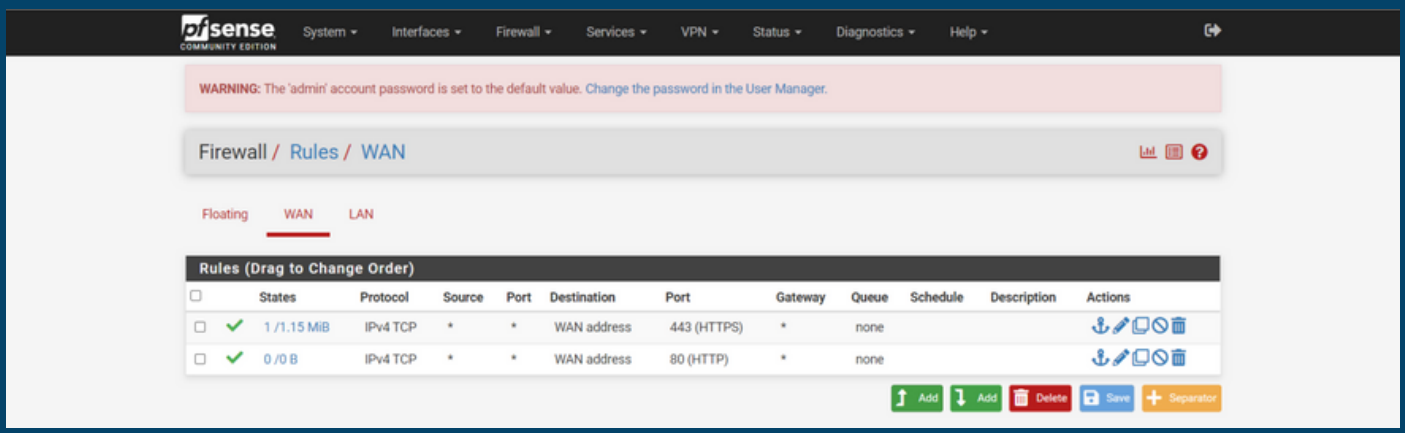
Utilisation de pfSense



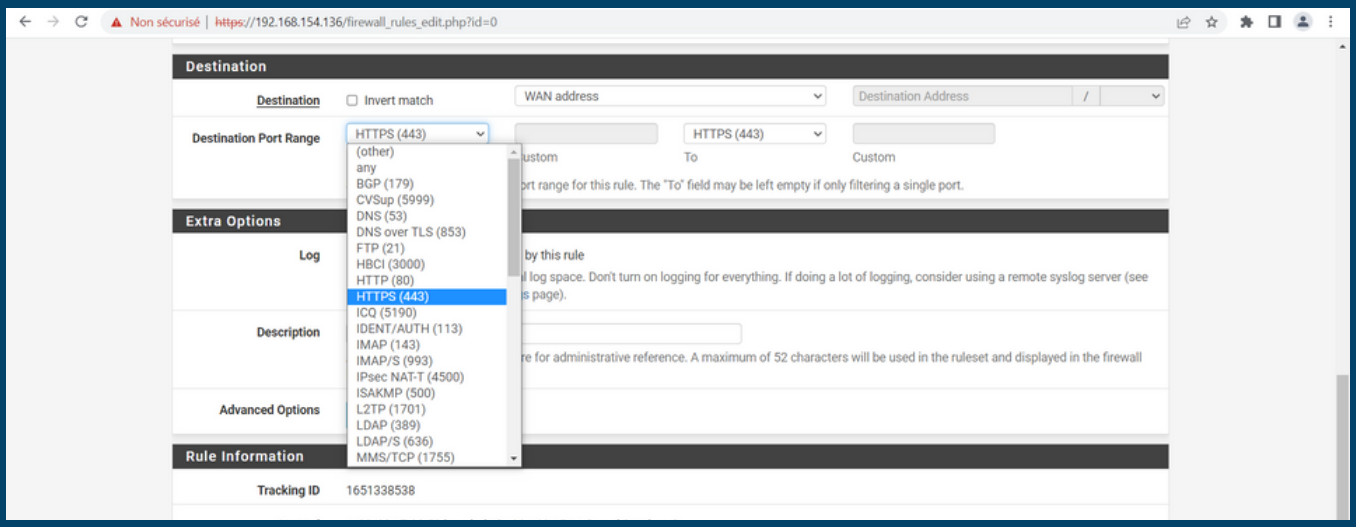
Page accueil pfSense



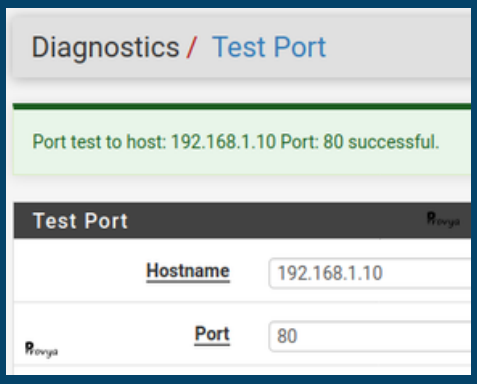
Gestion du pare-feu, "Rules"



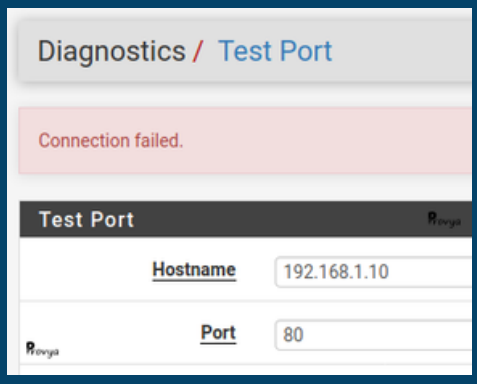
Gestion du WAN



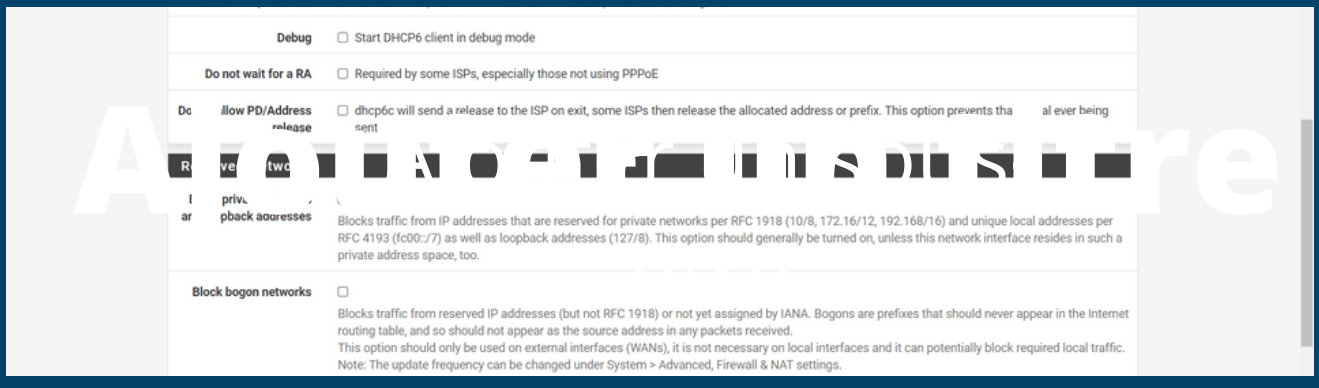
Choix du port HTTPS (sécurisé) Il faut s'assurer que le serveur cible soit bien en écoute sur le port de destination.
S'il s'agit d'un port TCP, on peut utiliser l'outil de test intégré à pfSense et accessible depuis le menu Diagnostics > Test Port :



Connexion réussie



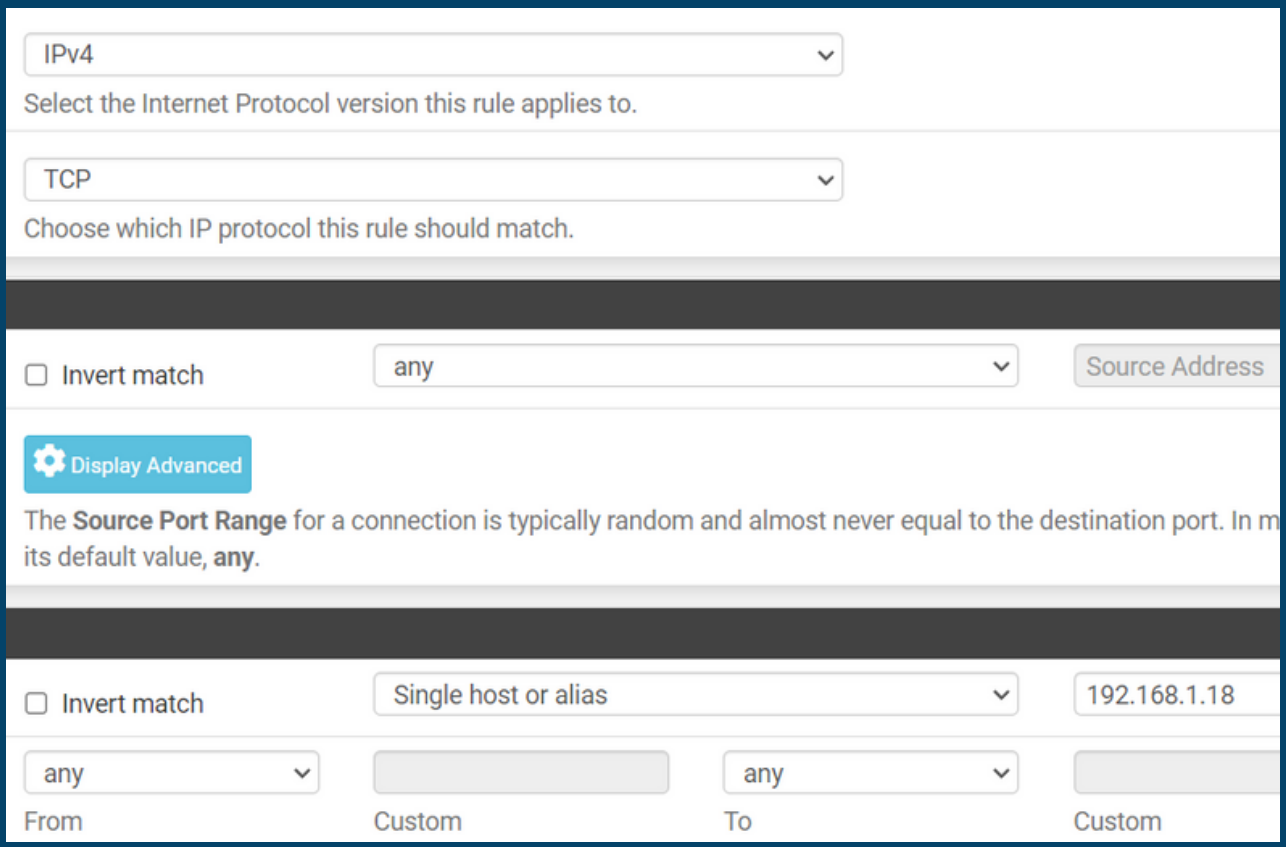
Connexion échouée



En bas de la page Interface -> Wan, décocher les cases "Bloquer réseaux privés et adresse de bouclage" (Une adresse de bouclage est une adresse utilisée par une interface pour s'envoyer un message à elle-même) et "Bloquer adresse bogon" (Un bogon est une adresse IP fausse provenant de l'espace bogon, qui est un ensemble d'adresses IP qui n'ont pas encore été officiellement attribuées à une entité par Internet). Cela permet d'avoir accès au site pfSense sans avoir besoin de la commande "pfctl -d"

Regle de filtrage

Dans les regles de filtrages du parefeu, on va mettre une regle de filtrage essentiel qui va ouvrir le port du serveur, pour que les connexions externe puissent accéder au site



SAUVEGARDE

Sauvegarde

Tout d'abord nous allons passer en utilisateur root et créer une clef publique et une clef privé ssh

```
sauvegarde@ubuntu:~$ sudo su root
[sudo] password for sauvegarde:
```

```
root@ubuntu:/home/sauvegarde# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
root@ubuntu:/home/sauvegarde# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:glYg2zQ7I9Zwd3wPQ8Xq7Gu4IhNVO8bEE5t4BVsi/A0 root@ubuntu
The key's randomart image is:
+---[RSA 3072]----+
|  o =.oo=++o.    |
|   O =.+EB+ .    |
|  + * o==* =     |
| . . =..* o .    |
|    o...S+       |
|   ..  .  o      |
|     .   o       |
|    o . . o      |
|     o ..o..     |
+----[SHA256]-----+
```

La clef publique est envoyé sur le serveur apache tandis que la clef privé va resté sur la vm du serveur de sauvegarde.
Grace a la clef publique qui va servir de relai pour envoyer des informations chiffré, dans notre cas, ça sera des fichiers de backup, et la clef privé va permettre de recevoir les fichiers et les déchiffrés.

Puis ensuite nous allons effectuer le script

```
Nouveaufichier="backup_$(date +%Y-%m-%d_%T)"
mkdir /home/sauvegarde/backup/$Nouveaufichier
scp apache@192.168.1.18:/var/www/html/index.css /home/sauvegarde/backup/$Nouveau
scp apache@192.168.1.18:/var/www/html/index.html /home/sauvegarde/backup/$Nouvea
```

C'est un script classique bash, pour effectuer le transfert de donnés du dossier ou les données du serveur apache sont stockés, jusqu'au dossier voulu sur la vm du serveur de sauvegarde.

Enfin nous allons automatiser cela grace à crontab, qui va executer le script de transfert de fichier toutes les 3 heures.

Crontab est un outil qui permet l'exécution de tache tout les x temps, le temp est décidé par les étoiles au début du crontab.

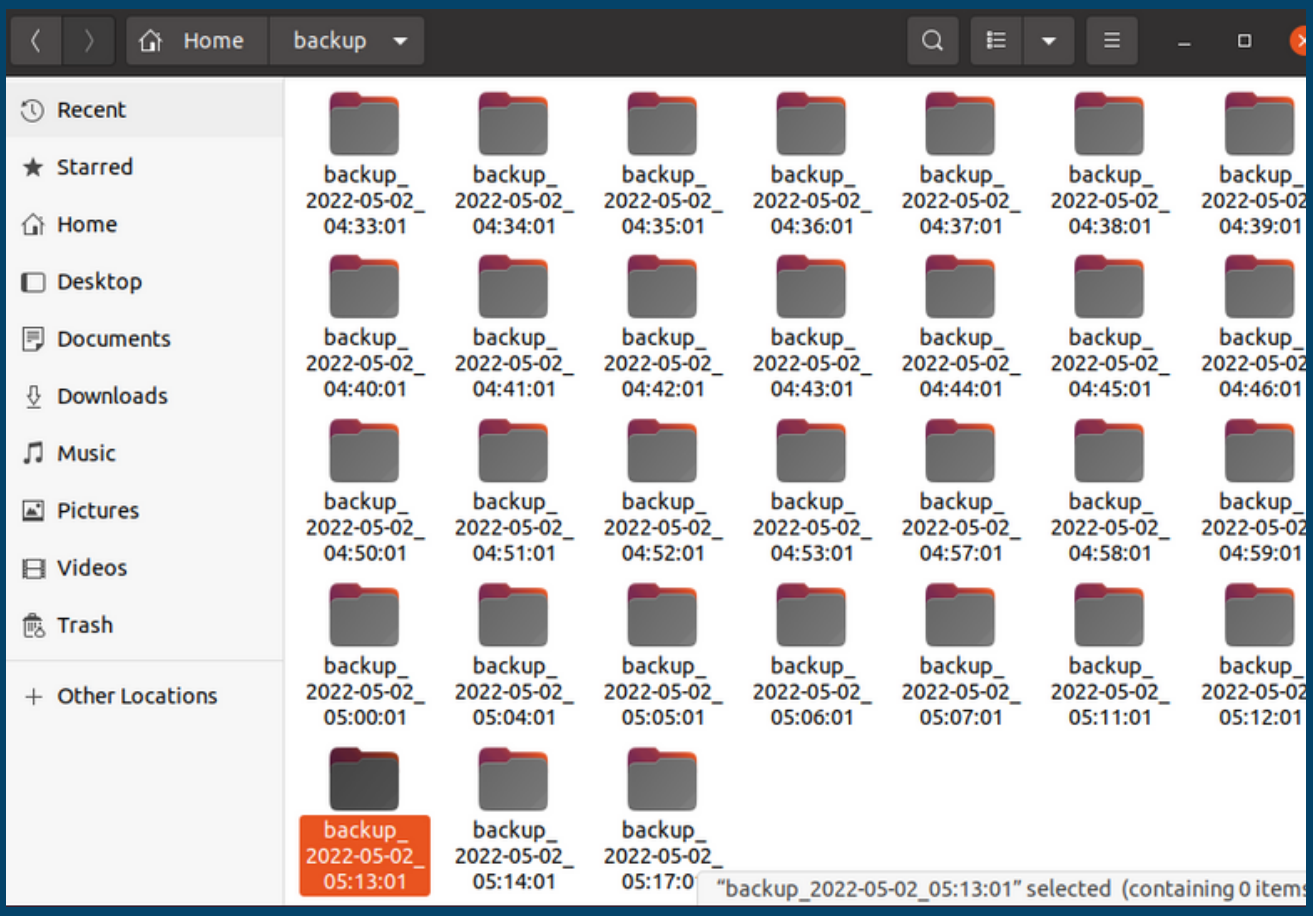
```
For more information see the manual pages of crontab(5) and cron(8)

m h  dom mon dow   command

*/3 * * * bash /home/sauvegarde/backup.sh
```

Restauration

La restauration sera faite tout simplement grâce au fichier de sauvegarde stocké dans le dossier situé dans la VM sauvegarde:/home/sauvegarde/backup
Grace au Crontab qui va créer un nouveau dossier toute les 3heures, on va pouvoir prendre n'importe qu'elle fichier selon la date et l'heure voulu.



Ensuite dans le dossier, il y aura un fichier css et un fichier html et donc pour la restauration, nous allons prendre ces fichiers et les mettres dans le dossier source du serveur apache situé : /var/www/html .