NAT

-

PFSENSE

Installation et configuration

TANET Margaux

CPI 2024-2025

Table des matières

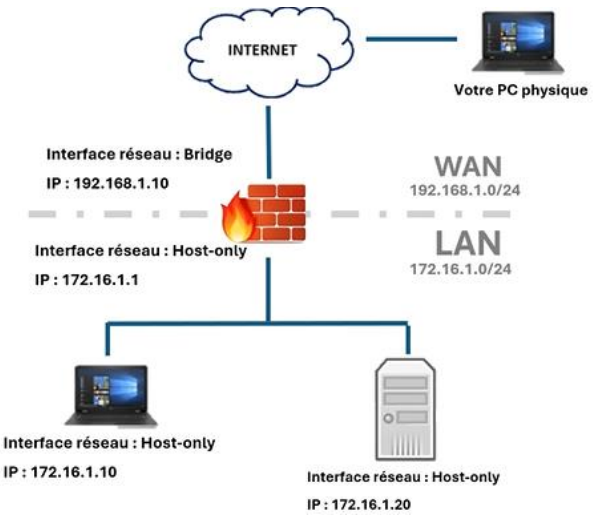
Pré requis :

- Avoir une VM Debian sans interface graphique avec NGINX pour le serveur web
- Avoir une VM PfSense avec deux cartes réseaux : WAN/LAN
- Avoir une VM Debian avec interface graphique qui nous servira à des fins de tests
- Avoir configurer les différentes interfaces et accéder au firewall en web depuis une VM Debian

Introduction :

Dans un premier temps, nous redirigerons le trafic venant de l'interface WAN sur le port 80 sur le serveur web. Nous donnerons un accès SSH à notre machine Debian qui héberge le site web. Par la suite, il faudra installer une Debian cliente sur la patte WAN de notre PfSense et nous testerons les ports ouverts sur notre firewall. Enfin, nous dissimulerons le SSH sur un port différent avec du PAT. Tout ceci sera montrer avec des tests.

Schéma réseau de notre infrastructure :



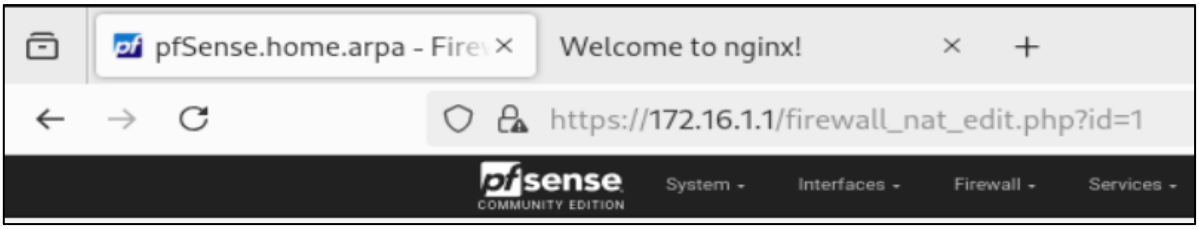
Configuration de mes différentes VM :

	Host Only	Bridged
Debian	172.16.1.10	
PfSense	172.16.1.1	192.168.1.10 (dans mon cas 192.168.40.134)
Serveur web Nginx	172.16.1.20	

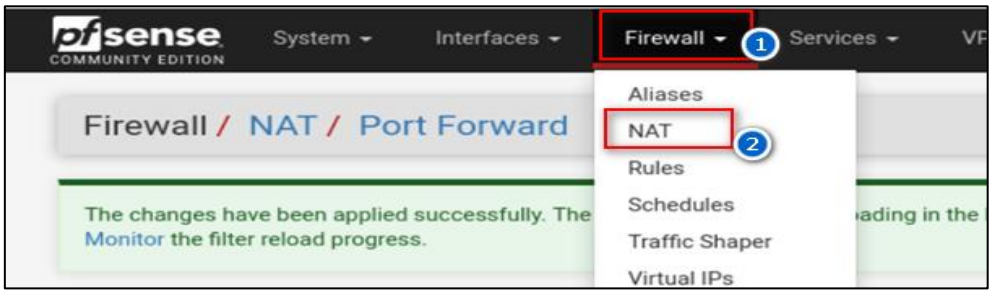
I- Mise en place de la redirection WAN vers le serveur web

a) Création de la règle de NAT

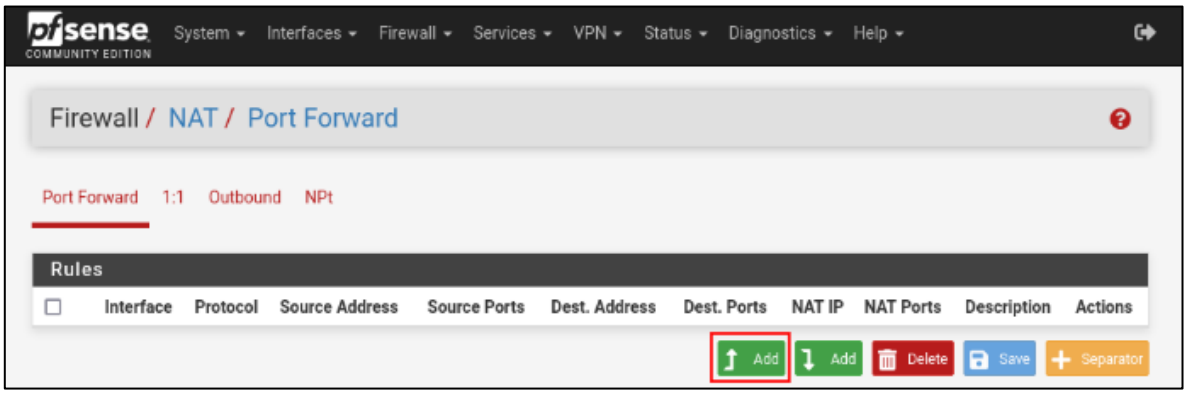
Pour faire la redirection du trafic de notre WAN sur le port 80 sur le serveur web, il faut se rendre sur notre VM Debian et taper **172.16.1.1** pour accéder en web à notre PfSense.



- Se rendre ensuite dans l'onglet **Firewall > NAT** :

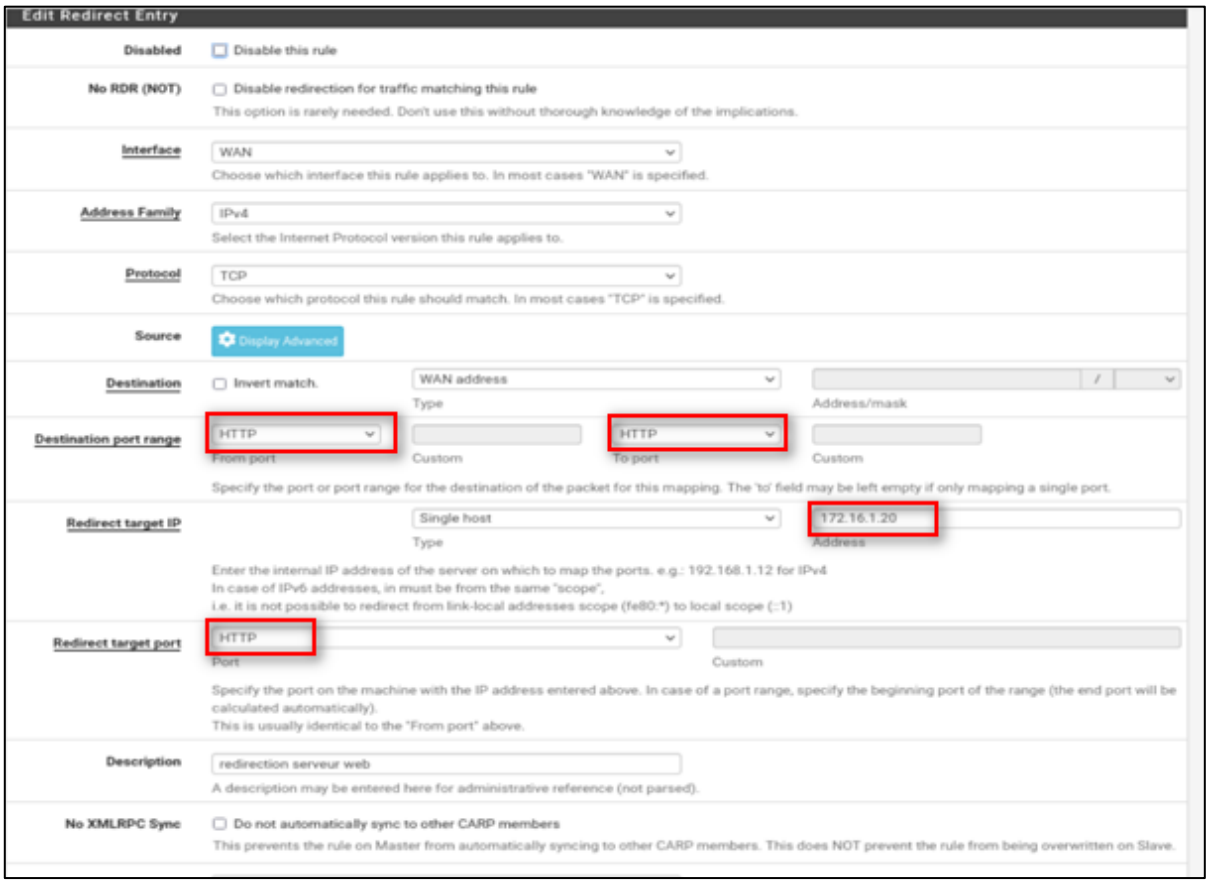


- Cliquer sur le bouton **Add** :

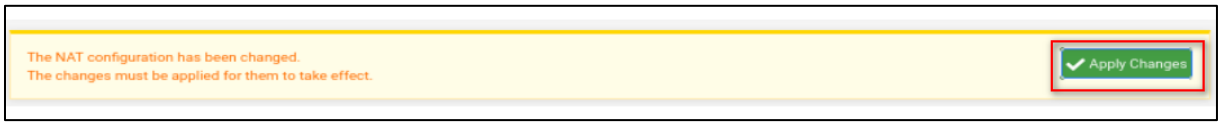


➢ Créer la règle de NAT :

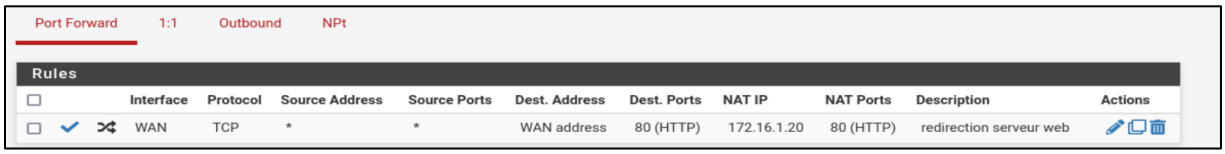
- **Port de destination :** WAN address
- **Destination port range** : HTTP = port 80
- **Redirect target IP** : single host / 172.16.1.20 (serveur web)
- **Redirect target port :** HTTP



➢ Appliquer les changements :

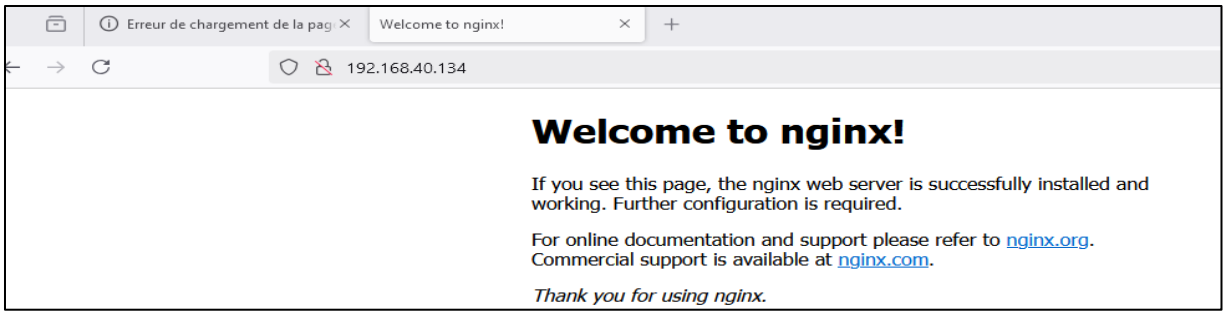


Notre règle de NAT est créée :



b) Test de la redirection

➢ Se rendre sur la VM Debian, depuis l'interface web, et taper l'IP **192.168.1.10** qui est l'accès à mon PfSense en WAN :



Pour des problèmes de connexion, je suis repassée en NAT pour récupérer une adresse en 192.168.40.134 car l'adresse IP 192.168.1.10 ne fonctionnait pas.

II- Mise en place d'un accès SSH à la machine Debian vers le serveur web

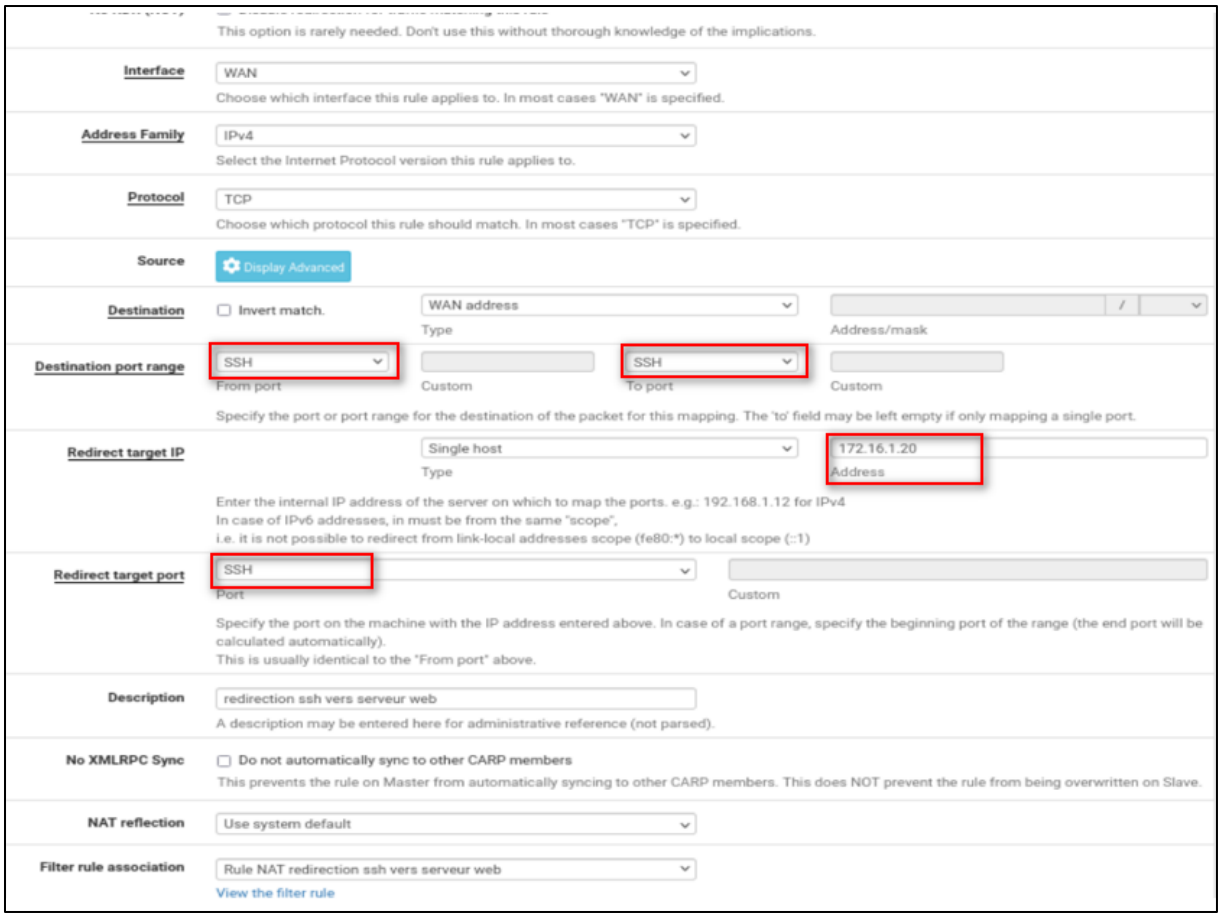
Avant de réaliser toutes actions, il faut avoir installé au préalable le paquet SSH sur mon serveur web pour que cela fonctionne. Faire la commande **apt install openssh-server**.

a) Création de la règle de NAT

- Se rendre ensuite sur ma machine Debian en interface web. Sur **l'interface web PfSense**, se rendre dans **Firewall > NAT** pour créer une règle pour le port 22 (port 22= SSH) :

Paramètre de la règle :

- **Destination port** range : SSH
- **Redirect target IP :** 172.16.1.20 (serveur web)
- **Redirect target port** : SSH

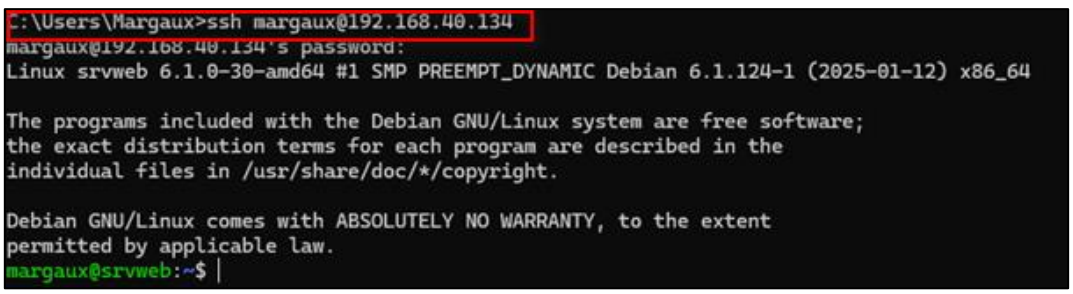


Cela va permettre un accès SSH à notre machine Debian depuis l'extérieur de notre réseau local.

b) Test pour la connexion en SSH

Nous allons tenter de nous connecter en SSH depuis notre machine hôte vers notre serveur web.

- Se rendre dans l'invite de commande, taper la commande suivante : **ssh utilisateur@ip_serveur_pfsense**

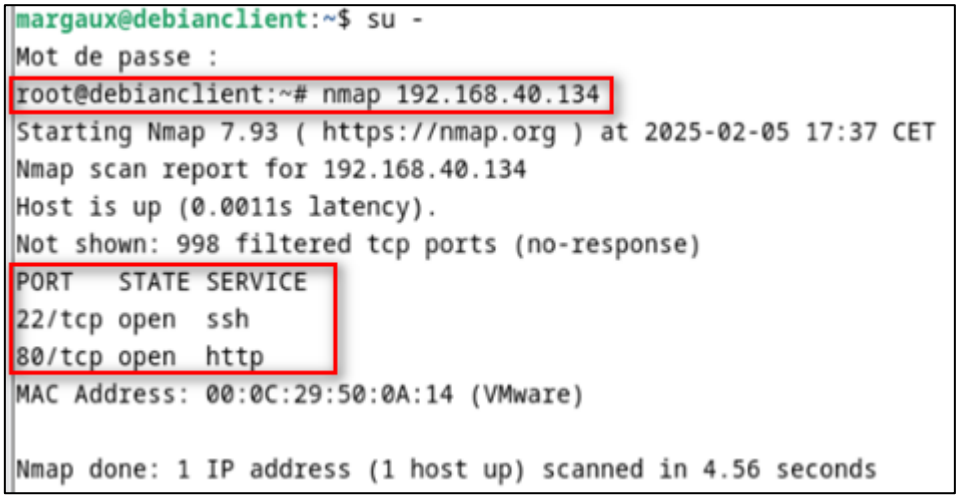


Nous arrivons à nous connecter à notre serveur web depuis notre machine.

III- Configuration et tests nmap

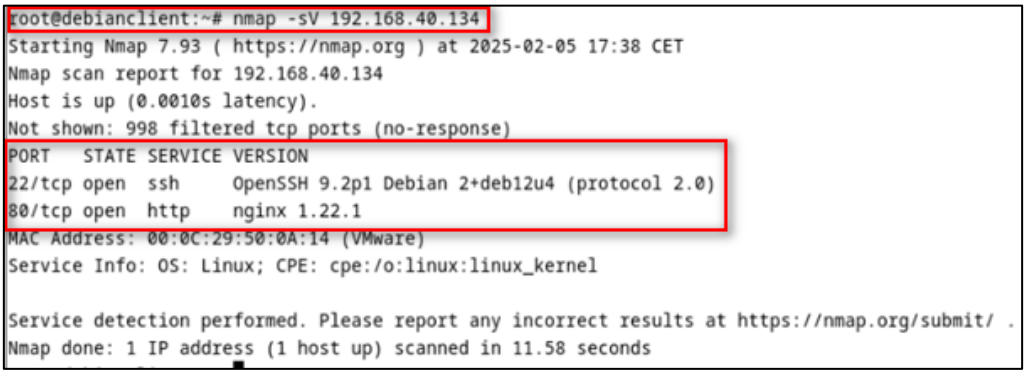
__Nmap__ est un outil de scan réseau utilisé pour voir les machines et services sur le réseau. Il communique des informations concernant les ports ouverts, services en cours d'exécution et bien plus.

- Il faut installer une nouvelle Debian sur la patte WAN (bridged) de notre PfSense. Il faut au préalable avoir installé le paquet **nmap**. La commande est la suivante : **apt install nmap**. Une fois cela réalisé, nous allons tester les ports ouverts sur notre firewall.
- Se rendre dans le terminal de la Debian créée précédemment et tapé : **nmap ip_pfsense**



On peut voir que les ports ouverts (SSH et HTTP) sont les deux ports que nous avons autorisées sur notre pare-feu.

De plus, nous pouvons savoir quels services tournent sur ces ports ainsi que la version exacte de ces services avec cette commande : **nmap -sV ip_pfsense**



On peut voir qu'OpenSSH et Nginx y sont présents.

IV- Dissimulation du SSH avec du PAT

Le **PAT** permet de rediriger un port externe vers un autre port interne sur une machine.

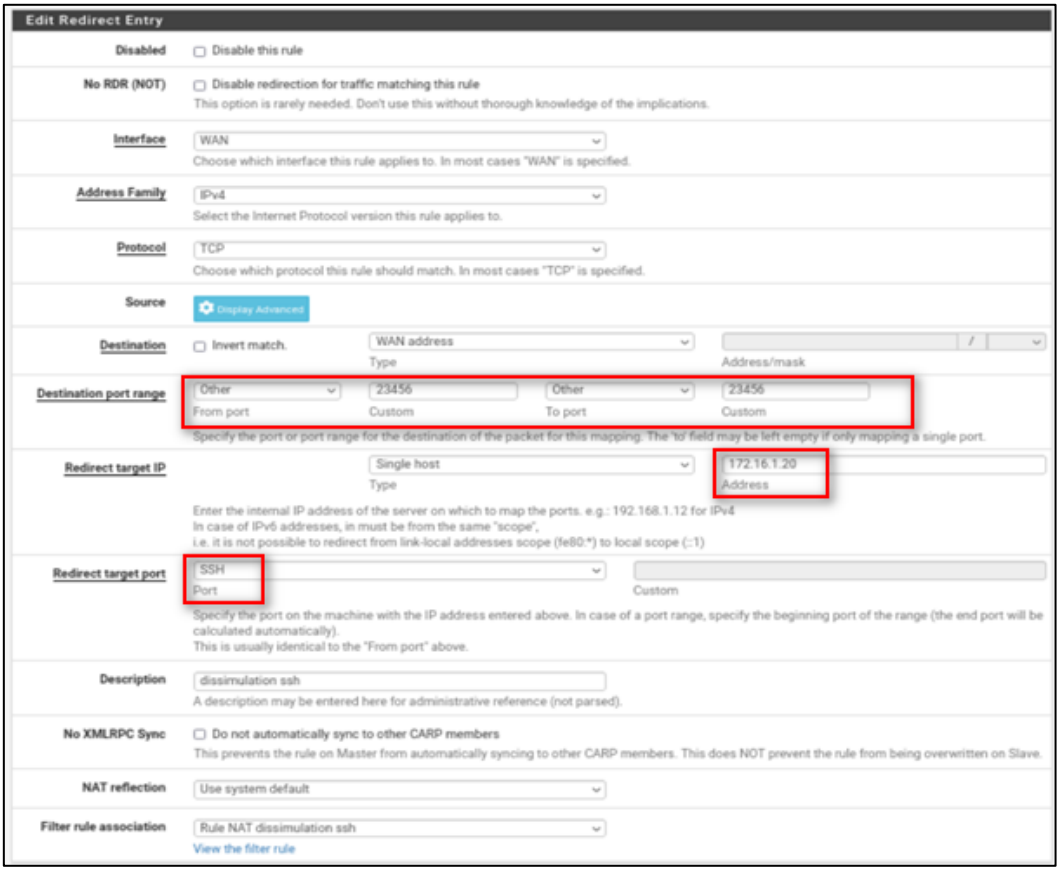
Pourquoi mettre en place du SSH avec du PAT ?

Par défaut, SSH écoute sur le port 22. Il est donc régulièrement scanné pour tenter des intrusions. C'est pour cela que couramment, on redirige un port externe vers le port interne 22.

Se rendre sur notre Debian en interface web et créer une nouvelle règle NAT :

Paramètre de la règle :

- **Destination port range :** other / 23456
- **Redirect target IP :** 172.16.1.20
- **Redirect target port :** SSH



⚠ **Attention :** ne pas oublier de désactiver la règle SSH port 22 pour qu'elle n'entre pas en conflit avec la nouvelle même si celle-ci continuerait de fonctionner :

➢ La commande **ssh utilisateur@ip_pfsense -p 22** permet de se connecter en SSH sur le port 22.

Cependant, nous venons de désactiver la règle de NAT qui autorise les connexions via le port donc nous devrions avoir une erreur :

```
C:\Users\Margaux>ssh margaux@192.168.40.134 -p 22
ssh: connect to host 192.168.40.134 port 22: Connection timed out
```

La connexion a échoué, la règle a bien été désactivée.

Nous testons la même commande mais cette fois-ci avec le nouveau port que l'on a appliqué dans la règle de NAT c'est-à-dire le port **23456** :

```
C:\Users\Margaux>ssh margaux@192.168.40.134 -p 23456
margaux@192.168.40.134's password:
Linux srvweb 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb  5 17:05:55 2025 from 192.168.40.1
margaux@srvweb:~$
```

Grâce à cette règle de NAT mise en place, toutes les connexions venant de l'extérieur utiliseront le port d'entrée **23456** où PfSense redirigera ensuite vers le port 22.

Voici le test réalisé depuis un pc client, la connexion est réussie :

```
root@debianclient:~# ssh margaux@192.168.40.134 -p 23456
margaux@192.168.40.134's password:
Linux srvweb 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb  5 22:04:50 2025 from 192.168.40.135
```

V- Conclusion

Dans ce document, nous avons vu la configuration de plusieurs règles NAT pour la redirection WAN vers le serveur web et l'accès en SSH. Nous avons scanner PfSense afin de voir les différents ports ouverts. Enfin, nous avons vu comment utiliser du PAT afin de rediriger notre port externe vers le port interne 22 pour éviter des scans basiques, attaques par brute-force qui restent le plus courant, par exemple.