

NAT - PFSENSE

Installation et configuration



TANET Margaux

CPI 2024-2025

Table des matières

I-	Mise en place de la redirection WAN vers le serveur web	3
a)	Création de la règle de NAT.....	3
b)	Test de la redirection	4
II-	Mise en place d'un accès SSH à la machine Debian vers le serveur web	5
a)	Création de la règle de NAT.....	5
b)	Test pour la connexion en SSH.....	6
III-	Configuration et tests nmap	7
IV-	Dissimulation du SSH avec du PAT.....	8
V-	Conclusion.....	9

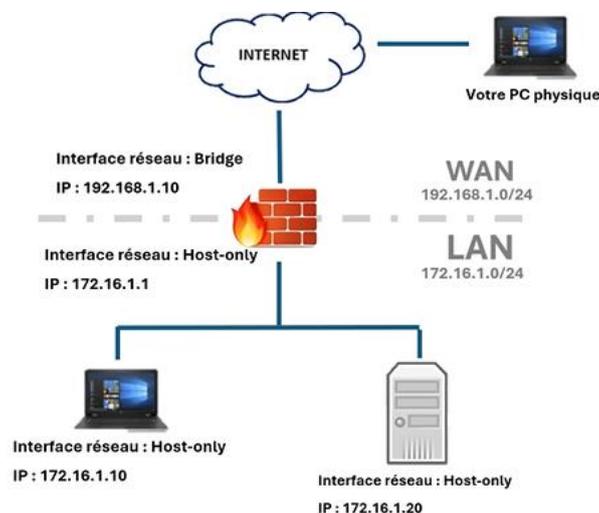
Pré requis :

- 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 configuré 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 montré avec des tests.

Schéma réseau de notre infrastructure :



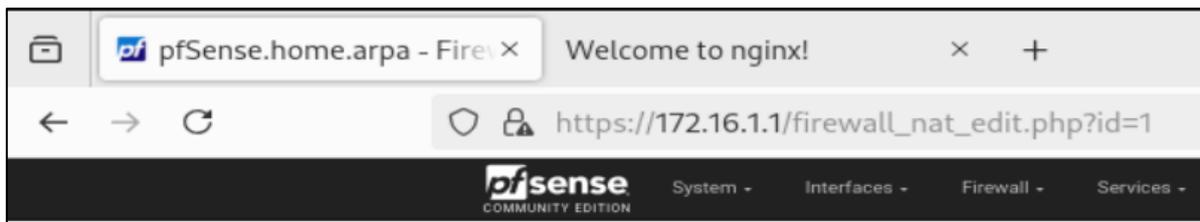
Configuration de mes différentes VM :

	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	

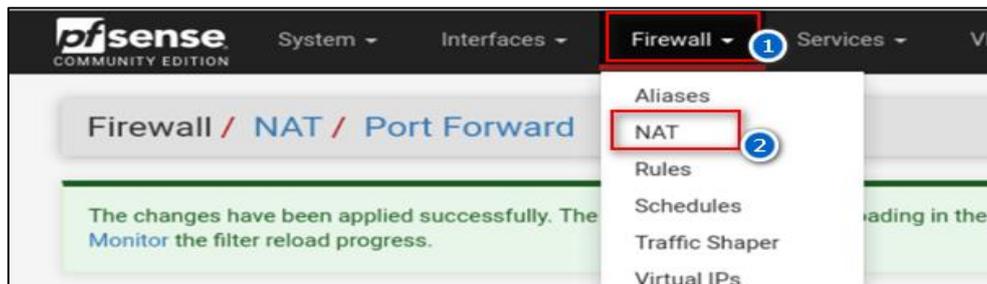
I- Mise en place de la redirection WAN vers le serveur web

a) Création de la règle de NAT

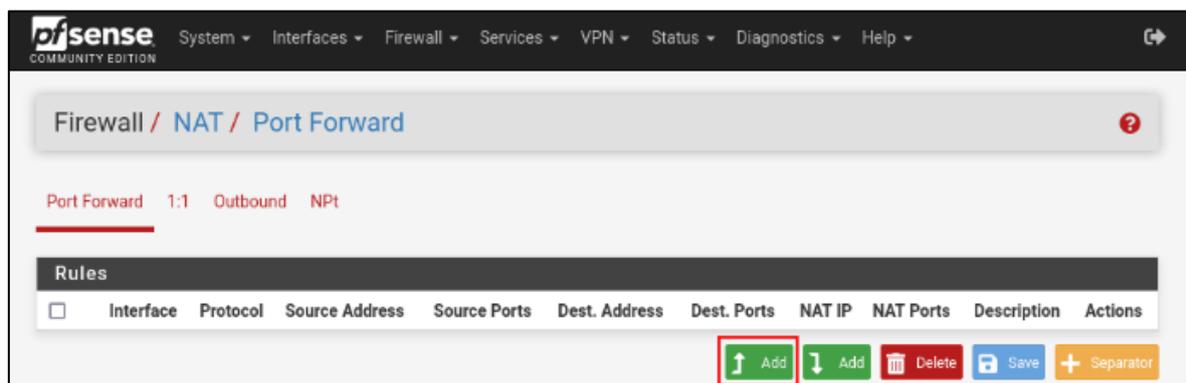
Pour faire la redirection du trafic de notre WAN sur le port 80 sur le serveur web, il faut se rendre sur notre VM Debian et taper **172.16.1.1** pour accéder en web à notre PfSense.



➤ 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

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination Invert match. WAN address
Type Address/mask

Destination port range HTTP
From port Custom HTTP
To port Custom
Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.

Redirect target IP Single host
Type 172.16.1.20
Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (-1)

Redirect target port HTTP
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description redirection serveur web
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

- Appliquer les changements :

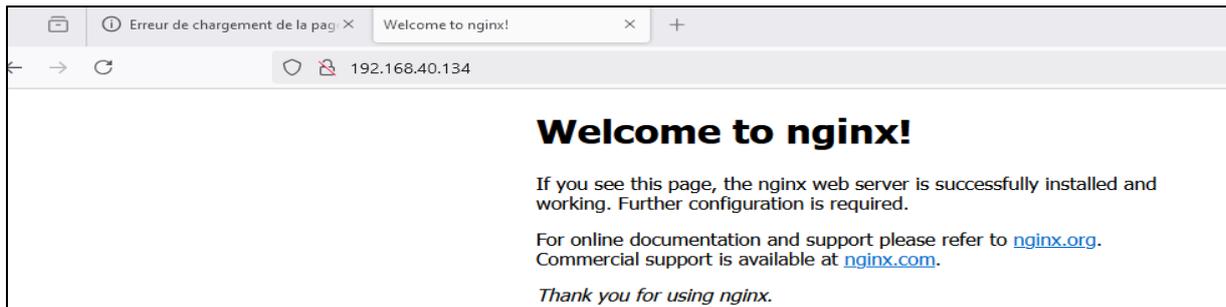
The NAT configuration has been changed.
The changes must be applied for them to take effect.

Notre règle de NAT est créée :

Port Forward		1:1	Outbound	NPt						
Rules										
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	172.16.1.20	80 (HTTP)	redirection serveur web	<input type="button" value="edit"/> <input type="button" value="clone"/> <input type="button" value="delete"/>

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

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface	WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.	
Source	Display Advanced
Destination	<input type="checkbox"/> Invert match. WAN address
Type Address/mask	
Destination port range	SSH From port SSH To port
Custom Custom	
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.	
Redirect target IP	Single host 172.16.1.20
Type Address	
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)	
Redirect target port	SSH
Port Custom	
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.	
Description	redirection ssh vers serveur web
A description may be entered here for administrative reference (not parsed).	
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.	
NAT reflection	Use system default
Filter rule association	Rule NAT redirection ssh vers serveur web
View the filter rule	

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**

```
.: \Users\Margaux> ssh margaux@192.168.40.134
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.
margaux@srvweb:~$
```

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**

```
margaux@debianclient:~$ su -
Mot de passe :
root@debianclient:~# nmap 192.168.40.134
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-05 17:37 CET
Nmap scan report for 192.168.40.134
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:50:0A:14 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
```

On peut voir que les ports ouverts (SSH et HTTP) sont les deux ports que nous avons autorisés 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**

```
root@debianclient:~# nmap -sV 192.168.40.134
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-05 17:38 CET
Nmap scan report for 192.168.40.134
Host is up (0.0010s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
80/tcp    open  http     nginx 1.22.1
MAC Address: 00:0C:29:50:0A:14 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.58 seconds
```

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.