PFSENSE

FIREWALL

LUCA BONA

SOMMAIRE

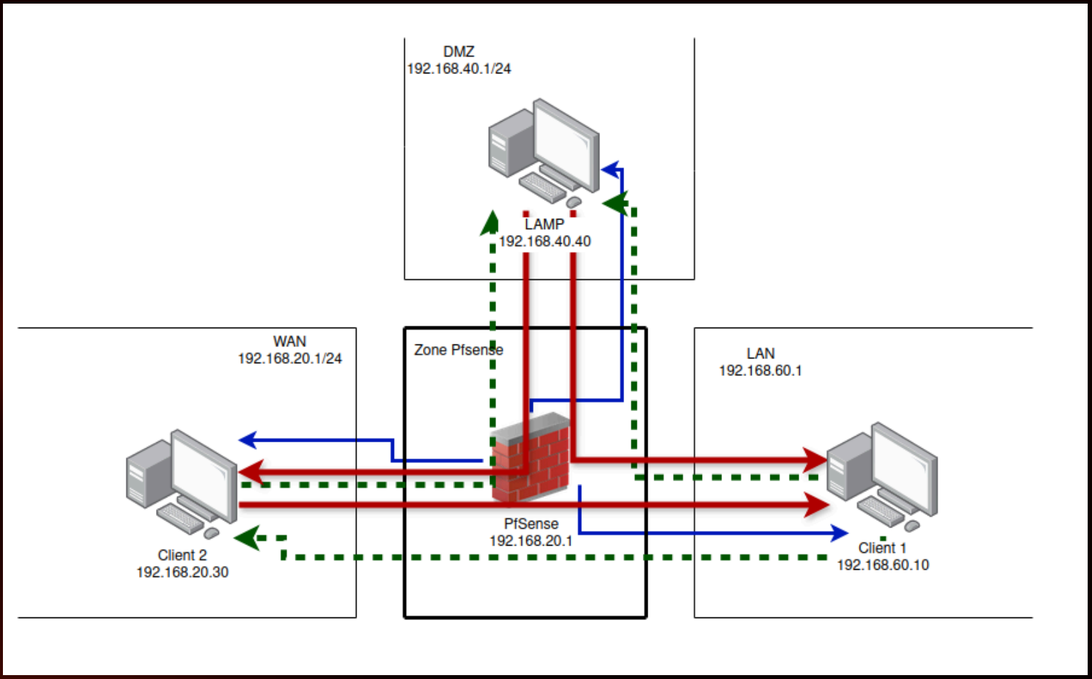
- QU’EST CE QUE PFSENSE
- INSTALLATION
- INTERFACE PFSENSE
- REGLE NAT
- DMZ - TEST
- LAN - TEST
- WAN - TEST
- RDP ET REGLE NAT
- ZABBIX
- ZABBIX - RESULTAT

LUCA BONA

QU'EST CE QUE PFSENSE

pfSense est un pare-feu/routeur open source basé sur FreeBSD.
Il offre du filtrage réseau, du VPN, du routage et des fonctions avancées comme la QoS ou le captive portal, le tout géré via une interface web.

Il permet aussi de gérer une DMZ (zone démilitarisée) : un sous-réseau isolé où l'on place des serveurs accessibles depuis Internet (web, mail, etc.), afin de protéger le réseau interne en cas de compromission.



Accès autorisé : la machine qui ping peut communiquer avec l'autre machine.

Lien entre les machines via pfSense (passerelle).

Accès non autorisé : la machine qui ping ne peut pas communiquer avec l'autre machine.

LUCA BONA

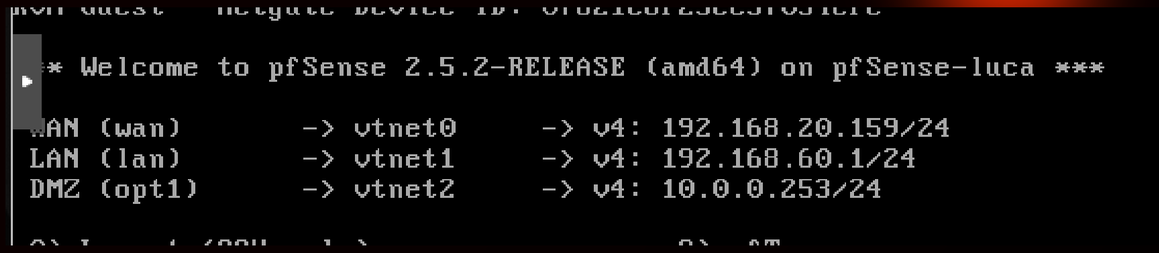
INSTALLATION

Lors de l'installation de pfSense, vous devriez avoir plusieurs cartes réseau.

Ici, j'utilise vmbr0 qui est mon lien WAN,
vmbr2 qui est mon lien DMZ,
et vmbr3 qui est mon lien LAN.

vmbr0	Linux Bridge	Yes	Yes	No	eno1	192.168.20.201/24	192.168.20.254	WAN pfsense
vmbr1	Linux Bridge	Yes	Yes	No	eno2	192.168.170.1/24		LAN pfsense
vmbr2	Linux Bridge	Yes	Yes	No	eno3	172.0.0.1/16		DMZ pfsense
vmbr3	Linux Bridge	Yes	Yes	No	eno4	192.168.60.201/24		LAN (perso)

Une fois l'installation faite, vous arriverez sur cette interface.



Modifiez les adresses IP de vos liens : évitez le DHCP et préférez utiliser des adresses IP fixes.

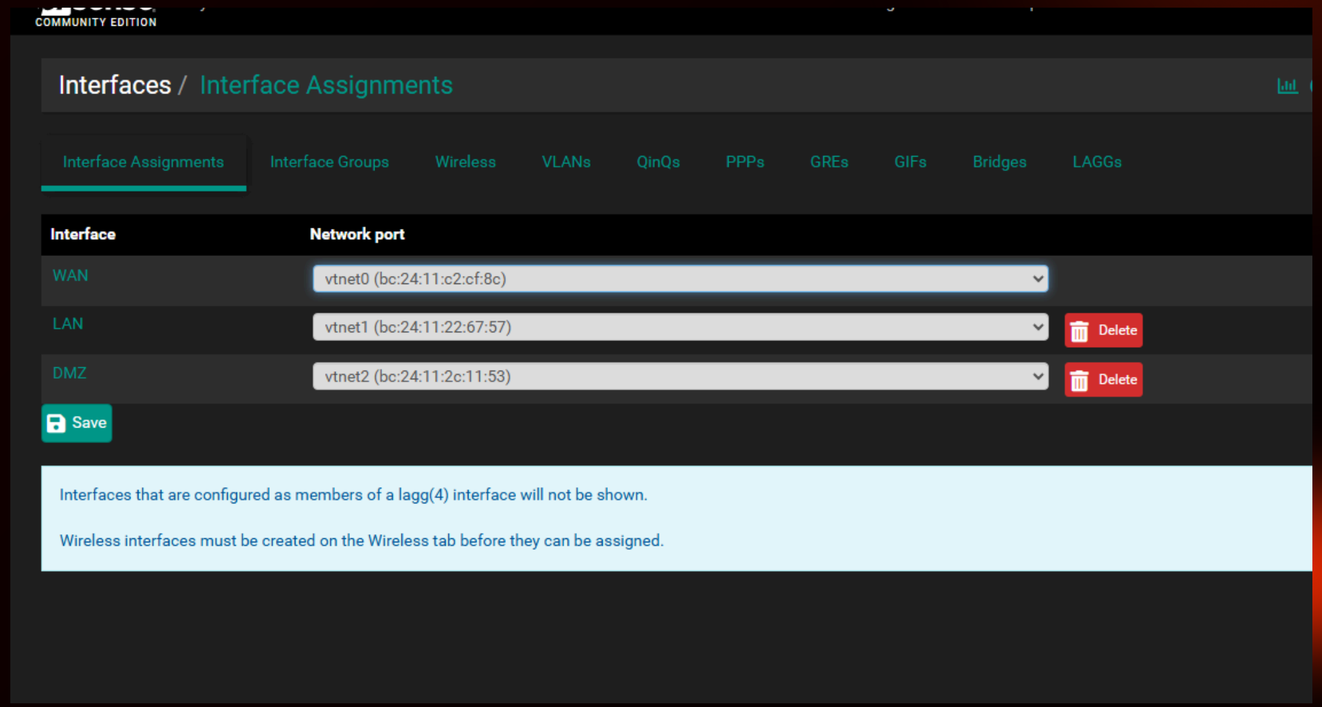
Dans mon réseau, sur le LAN j'utiliserai une machine Windows, et pour la DMZ, un serveur LAMP sous Debian.

INTERFACE PFSENSE

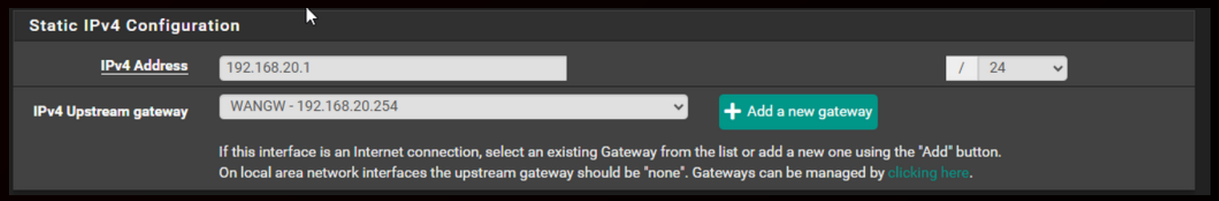
En local, saisissez l'adresse IP de votre pfSense (192.168.20.1) et vous arriverez sur une interface graphique (identifiant = admin, mot de passe = mdp VMpfsense).

Faites le Setup Wizard, puis nous allons commencer à définir des règles pour le pare-feu.

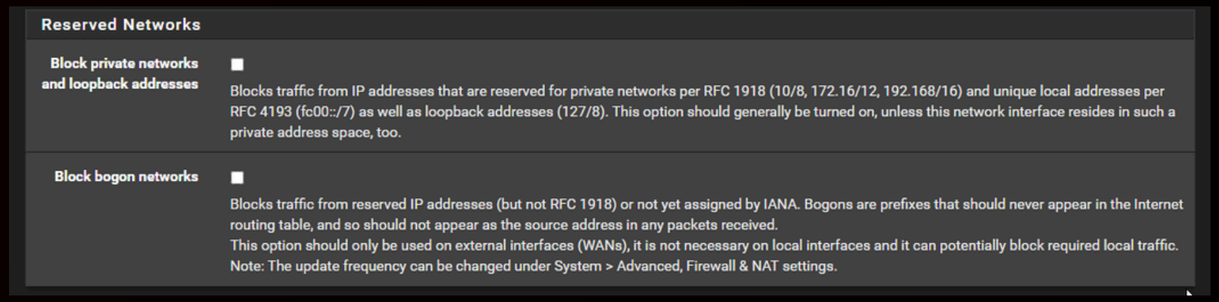
Ajoutez la DMZ en tant qu'interface (et, par la même occasion, vérifiez que les cartes réseau sont assignées aux bonnes interfaces).



Vérifiez et/ou ajoutez les adresses IP des interfaces : elles doivent être les mêmes que celles définies précédemment sur la VM pfSense.

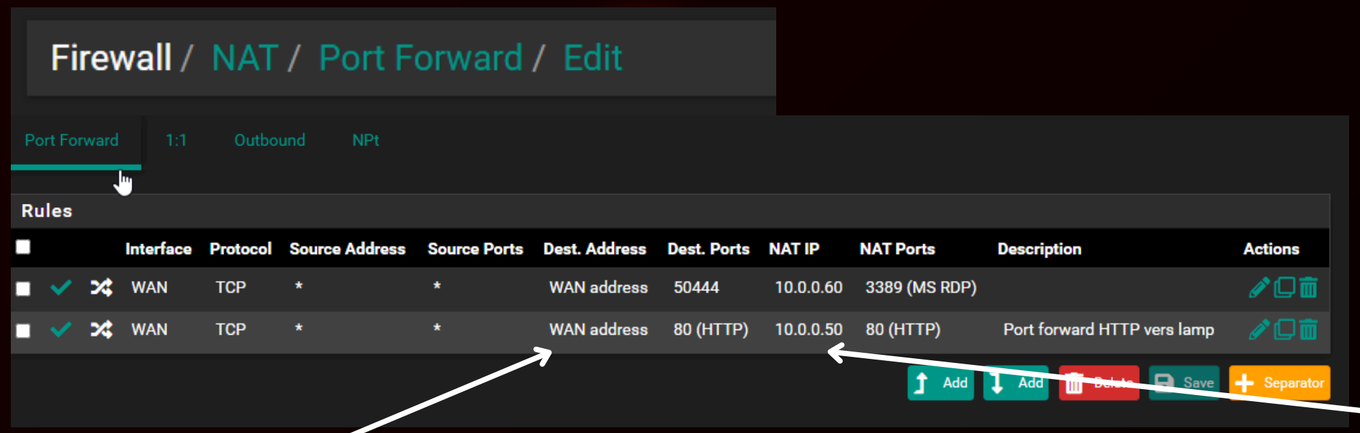


Décochez les deux cases dans Reserved Networks.



REGLE NAT

01



Dans le pare-feu, nous allons ajouter une règle NAT, qui permet de rediriger le trafic du WAN vers la DMZ. Pour faire simple, depuis le WAN, on utilise l'adresse IP de pfSense, qui redirige le trafic vers la DMZ.

10.0.0.50 étant l'IP de mon serveur LAMP situé dans la DMZ.

DMZ - TEST

Ping du Lamp de la DMZ vers la LAN

```
root@debian:/home/sio# ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
From 10.0.0.50 icmp_seq=10 Destination Host Unreachable
From 10.0.0.50 icmp_seq=11 Destination Host Unreachable
From 10.0.0.50 icmp_seq=12 Destination Host Unreachable
From 10.0.0.50 icmp_seq=13 Destination Host Unreachable
From 10.0.0.50 icmp_seq=14 Destination Host Unreachable
```

Ping du Lamp de la DMZ vers Pfsense

```
root@debian:/home/sio# ping 192.168.20.159
PING 192.168.20.159 (192.168.20.159) 56(84) bytes of data.
From 10.0.0.50 icmp_seq=1 Destination Host Unreachable
From 10.0.0.50 icmp_seq=2 Destination Host Unreachable
From 10.0.0.50 icmp_seq=3 Destination Host Unreachable
From 10.0.0.50 icmp_seq=4 Destination Host Unreachable
From 10.0.0.50 icmp_seq=5 Destination Host Unreachable
From 10.0.0.50 icmp_seq=8 Destination Host Unreachable
From 10.0.0.50 icmp_seq=9 Destination Host Unreachable
```

Ping du Lamp de la DMZ vers WAN

```
root@debian:/home/sio# ping 192.168.20.30
PING 192.168.20.30 (192.168.20.30) 56(84) bytes of data.
```

LAN - TEST

Accés du LAN a LA DMZ

Ping LAN vers DMZ

```
C:\Users\sio2025>ping 10.0.0.50

Envoi d'une requête 'Ping'  10.0.0.50 avec 32 octets de données :
Réponse de 10.0.0.50 : octets=32 temps=1 ms TTL=63
Réponse de 10.0.0.50 : octets=32 temps=1 ms TTL=63
Réponse de 10.0.0.50 : octets=32 temps=1 ms TTL=63
Réponse de 10.0.0.50 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 10.0.0.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Ping LAN vers WAN

```
C:\Users\sio2025>ping 192.168.20.30

Envoi d'une requête 'Ping'  192.168.20.30 avec 32 octets de données :
Réponse de 192.168.20.30 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.20.30 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.20.30 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.20.30 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 192.168.20.30:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

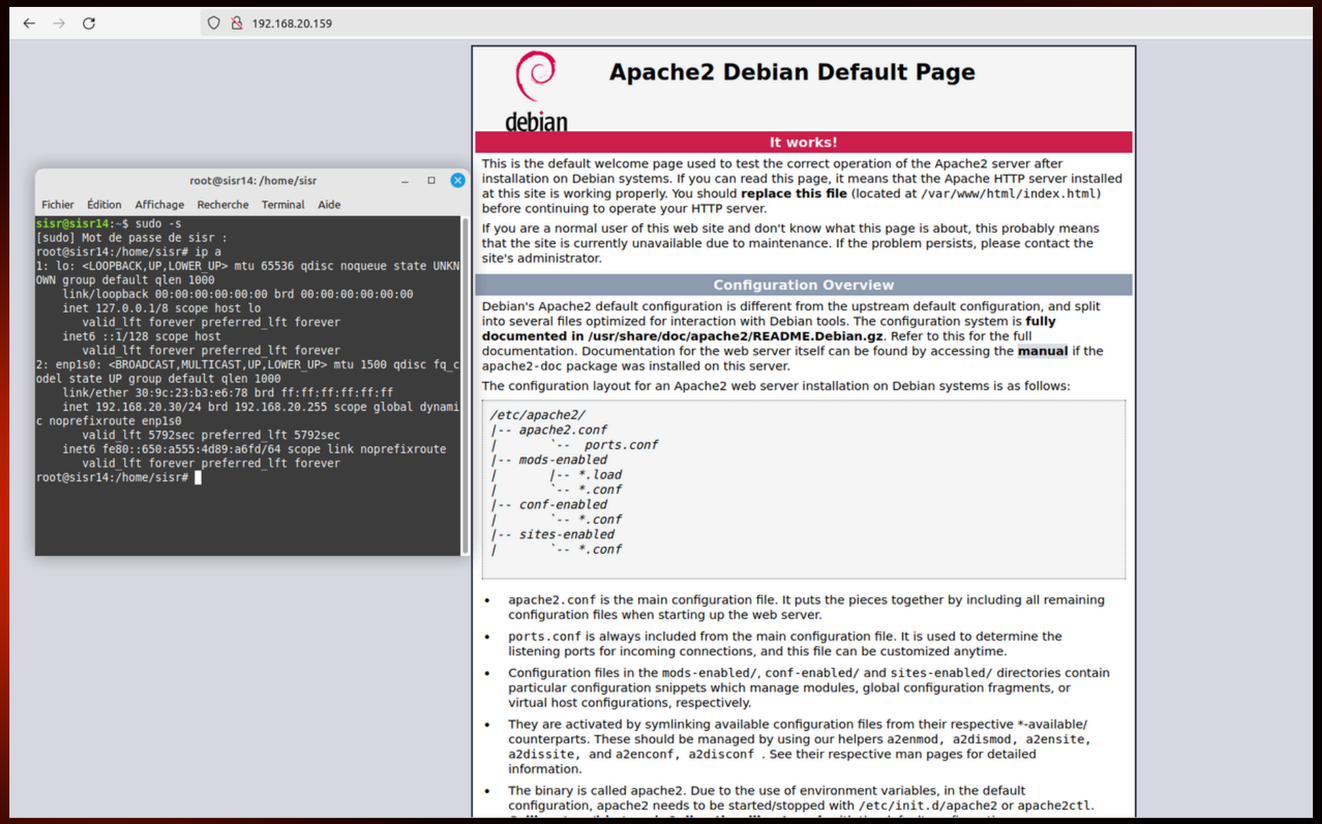
WAN - TEST

Ping du WAN vers DMZ

```
root@sisr14:/home/sisr# ping 10.0.0.50
PING 10.0.0.50 (10.0.0.50) 56(84) bytes of data.
```

Ping du WAN vers LAN

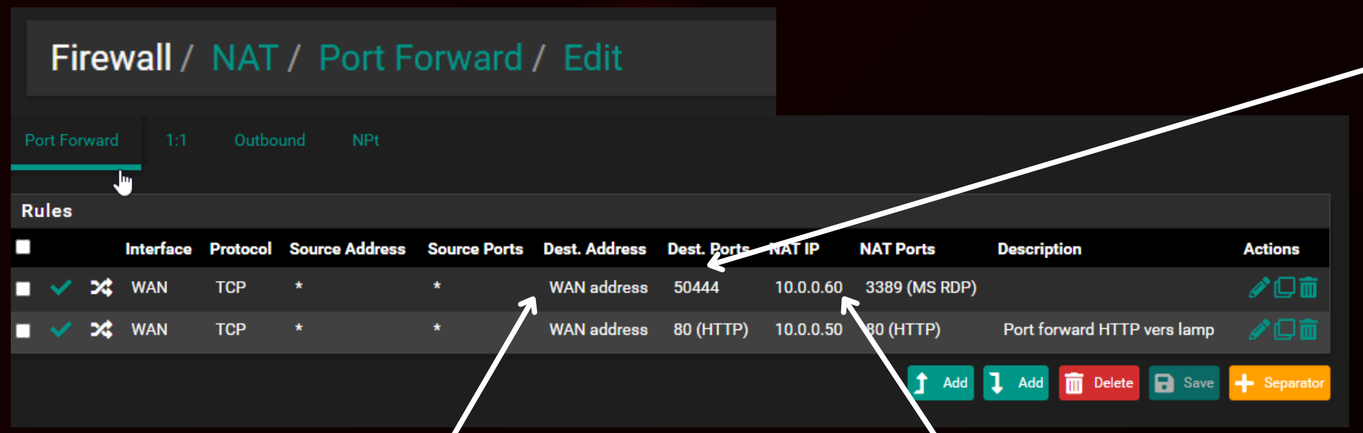
```
root@sisr14:/home/sisr# ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
```



Avec la règle NAT, j'ai accès à la page Web située dans la DMZ. Grâce à la redirection, en entrant l'adresse de pfSense, je suis automatiquement redirigé vers la DMZ.

RDP ET REGLE NAT

01



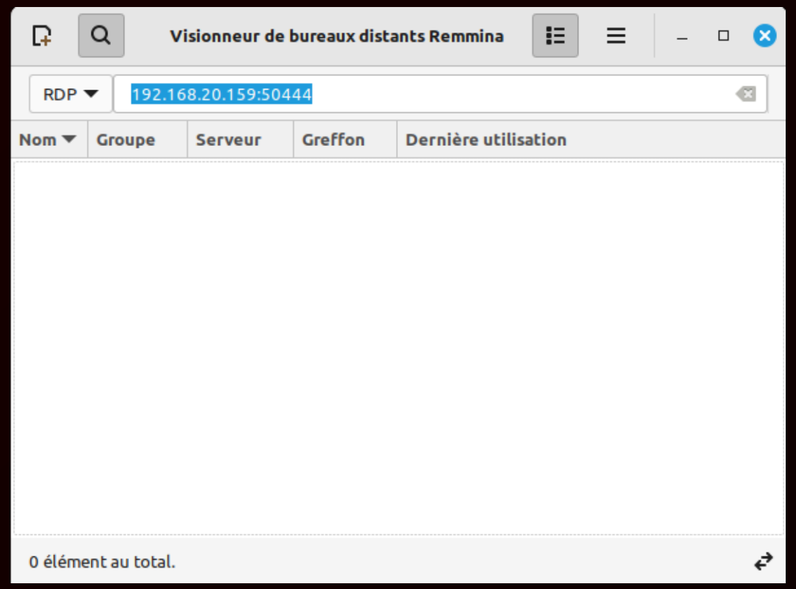
Le port de destination est “50444”, mais j’aurais pu mettre “49054” ou “83904”, peu importe, car le port RDP par défaut est le 3389 et l’utiliser tel quel peut représenter une faille de sécurité.

Pour profiter du RDP (Bureau à distance), nous allons créer une nouvelle règle qui permet de se connecter depuis le WAN au serveur Windows situé dans la DMZ.

10.0.0.60 étant l’IP de mon serveur Windows situé dans la DMZ.

01

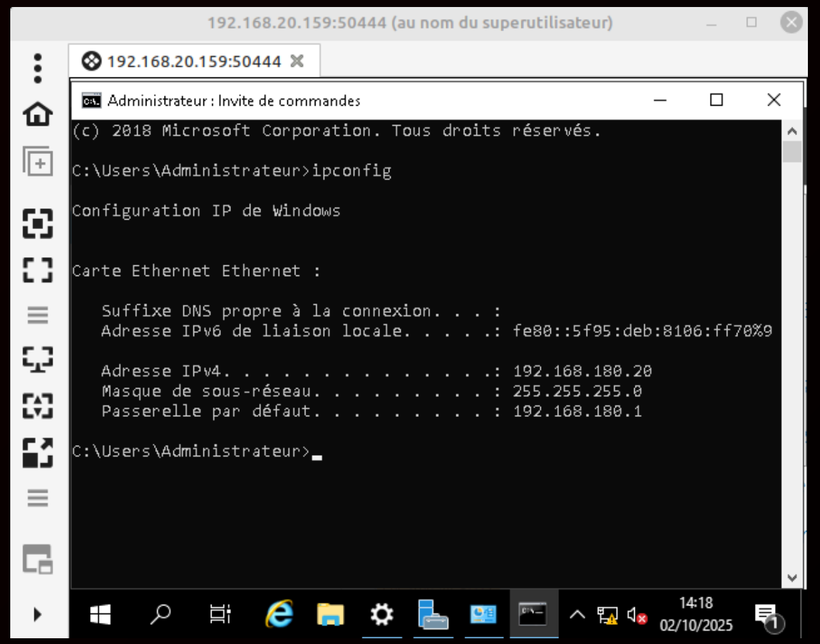
Avec Remmina, qui offre un accès au bureau à distance.



RDP

02

J'ai accès à mon serveur Windows depuis ma machine sur le WAN.



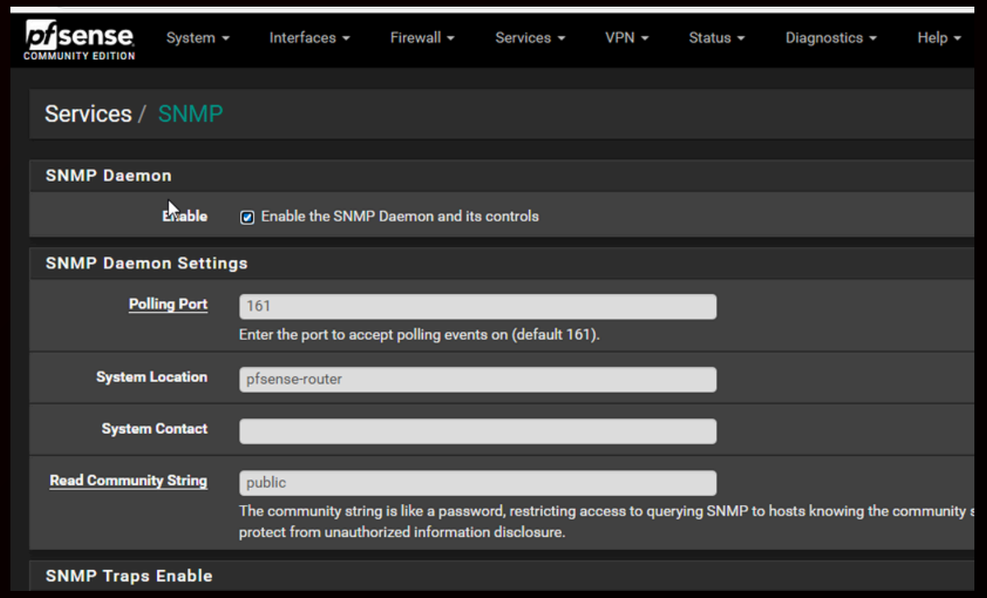
ZABBIX

01

La solution choisie pour surveiller pfSense est Zabbix, car elle est facile à installer et fonctionne très bien avec ce système. Elle permet de surveiller en temps réel l'état du pare-feu, comme l'utilisation du processeur, de la mémoire ou du trafic réseau. Zabbix peut également envoyer des alertes en cas de problème, par exemple si une interface tombe en panne. Son interface est claire et pratique, ce qui la rend adaptée pour contrôler et maintenir pfSense facilement.

02

Pour mettre en place cette supervision, il me faut un serveur Zabbix sur mon LAN. Ensuite, il faut configurer un nouvel hôte dans Zabbix pour pouvoir remonter les informations de pfSense. Avant de créer l'hôte, nous devons activer le SNMP sur pfSense. Le SNMP sert à surveiller et gérer à distance les équipements réseau, comme les routeurs, serveurs ou pare-feu, en collectant leurs informations de fonctionnement. C'est donc parfait pour assurer la continuité de service.

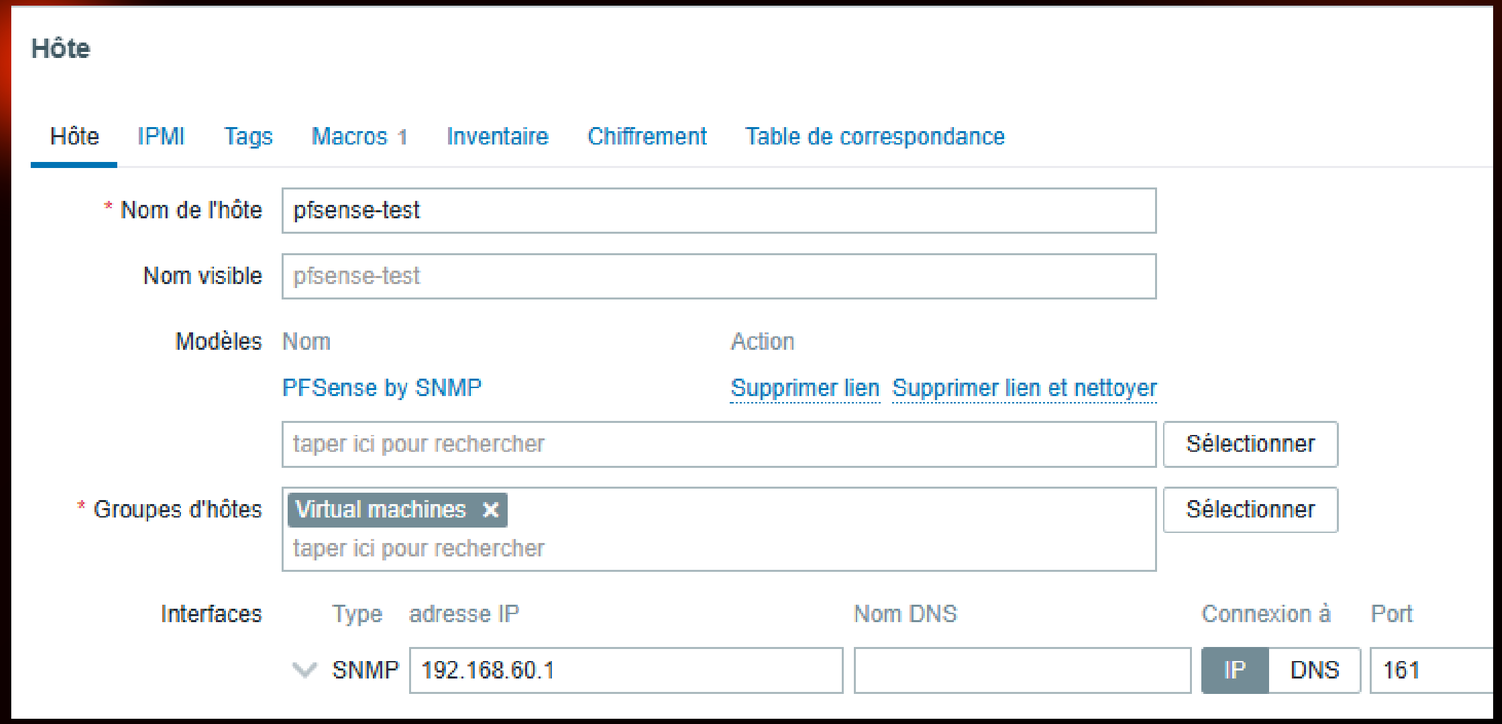


03

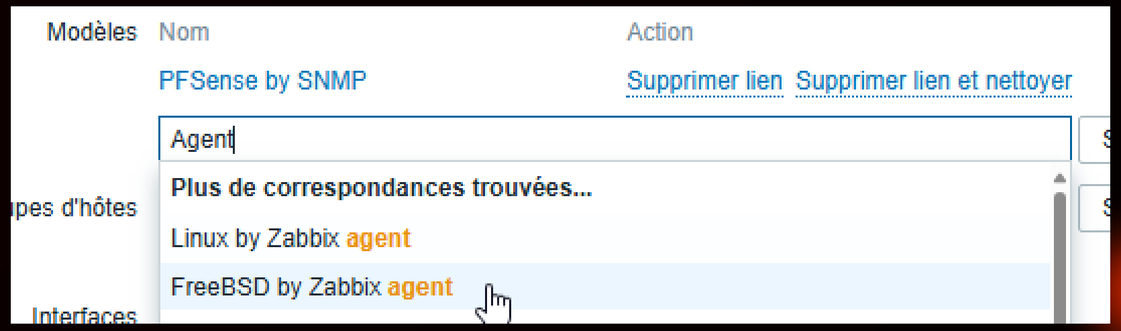
Ici, j'utilise le SNMP, mais j'aurais très bien pu utiliser l'agent Zabbix, à installer dans System > Package Manager. C'est un add-on que l'on installe soi-même.

ZABBIX

Lors de la création de l'hôte, si vous utilisez la méthode avec le SNMP, vous devez sélectionner dans Modèles : "pfSense by SNMP". Sans cela, aucune information, ni même un ping, ne pourra passer entre Zabbix et pfSense. Ensuite, il faut renseigner l'adresse IP LAN, et non celle utilisée pour accéder à l'interface graphique de pfSense. En résumé, vous devez mettre l'IP de votre LAN.



Si vous utilisez l'agent Zabbix installé en add-on sur pfSense, vous devez sélectionner "FreeBSD" dans Modèles.



ZABBIX - RESULTAT

Et mon PFSense est bien remonté