



# PFSENSE

FIREWALL

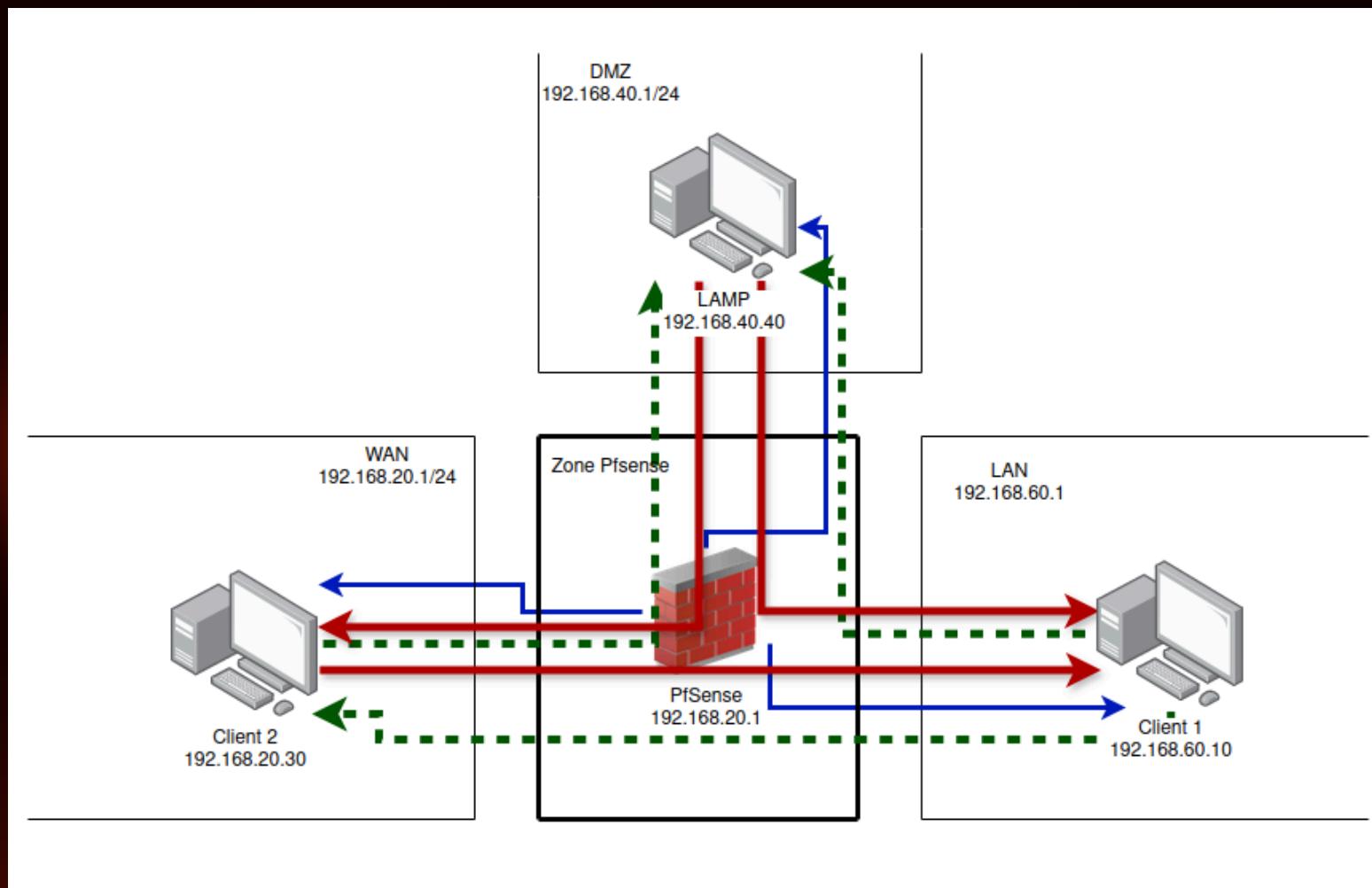
# SOMMAIRE

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

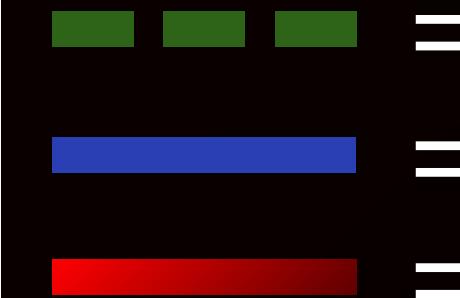


# QU'EST CE QUE PFSENSE

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.

# 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'utilisera une machine Windows, et pour la DMZ, un serveur LAMP sous Debian.

```
** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense-luca **

WAN (wan)      -> vtnet0      -> v4: 192.168.20.159/24
LAN (lan)      -> vtnet1      -> v4: 192.168.60.1/24
DMZ (opt1)     -> vtnet2      -> v4: 10.0.0.253/24
```

# 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.

Interfaces / Interface Assignments

Interface Assignments    Interface Groups    Wireless    VLANs    QinQs    PPPs    GREs    GIFs    Bridges    LAGGs

Interface	Network port
WAN	vtne0 (bc:24:11:c2:cf:8c)
LAN	vtne1 (bc:24:11:22:67:57)
DMZ	vtne2 (bc:24:11:2c:11:53)

**Save**

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Static IPv4 Configuration

IPv4 Address: 192.168.20.1 / 24

IPv4 Upstream gateway: WANGW - 192.168.20.254

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

**Block private networks and loopback addresses**  Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

**Block bogon networks**  Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

# REGLE NAT

01

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
■	WAN	TCP	*	*	WAN address	50444	10.0.0.60	3389 (MS RDP)		
■	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.50	80 (HTTP)	Port forward HTTP vers lamp	

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

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.

# 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
```

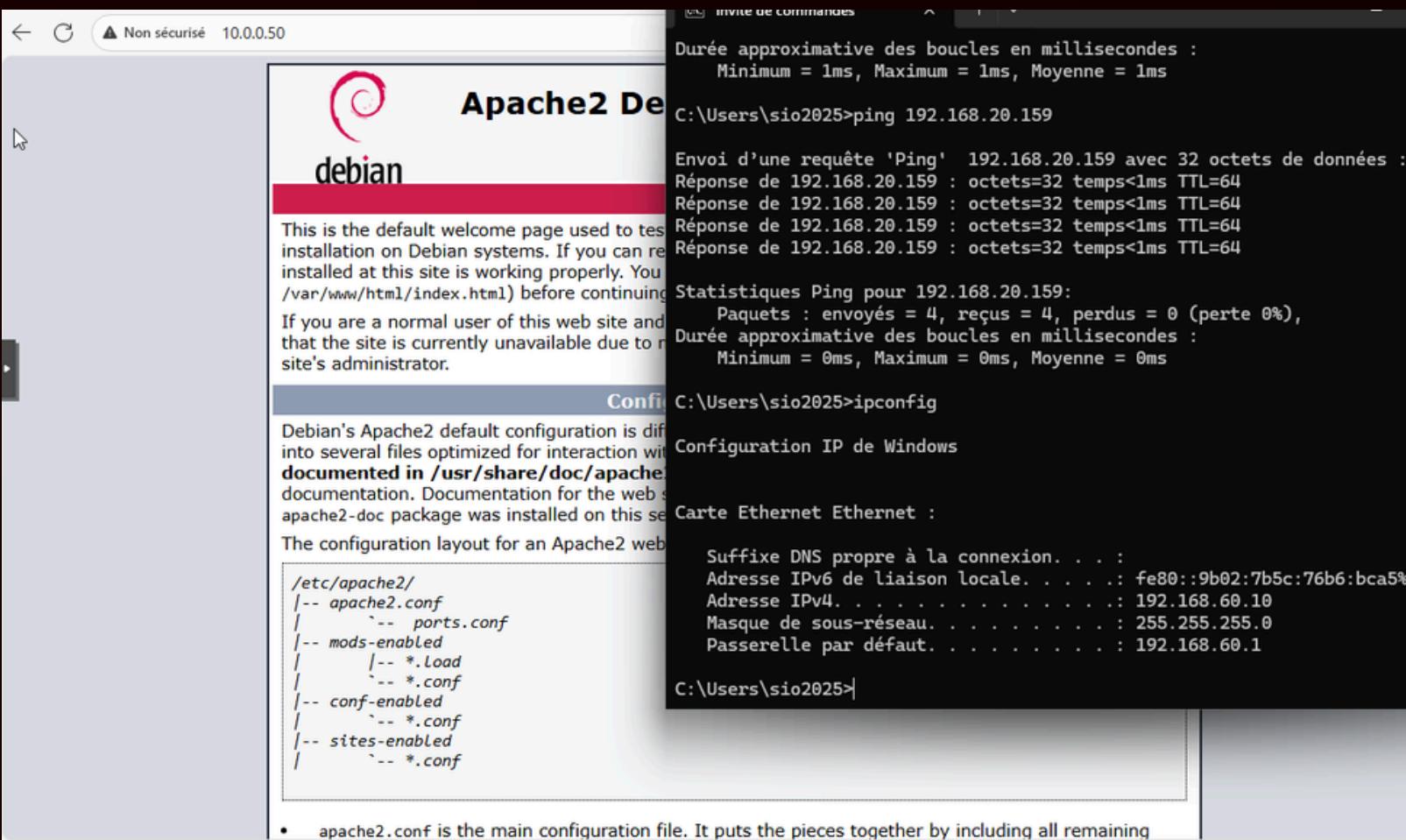
Ping du Lamp de la DMZ vers PfSense

```
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.
```

## Accès du LAN a LA DMZ



```

Durée approximative des boucles en millisecondes :
  Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
C:\Users\sio2025>ping 192.168.20.159
Envoi d'une requête 'Ping' 192.168.20.159 avec 32 octets de données :
Réponse de 192.168.20.159 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.20.159:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\sio2025>ipconfig
Configuration IP de Windows

Carte Ethernet Ethernet :
  Suffrage DNS propre à la connexion. . . . . :
  Adresse IPv6 de liaison locale. . . . . : fe80::9b02:7b5c:76b6:bca5%14
  Adresse IPv4. . . . . : 192.168.60.10
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 192.168.60.1

C:\Users\sio2025>

```

\* apache2.conf is the main configuration file. It puts the pieces together by including all remaining

Ping LAN vers DMZ

C:\Users\sio2025&gt;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

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

## LAN - TEST

Ping LAN vers WAN

C:\Users\sio2025&gt;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

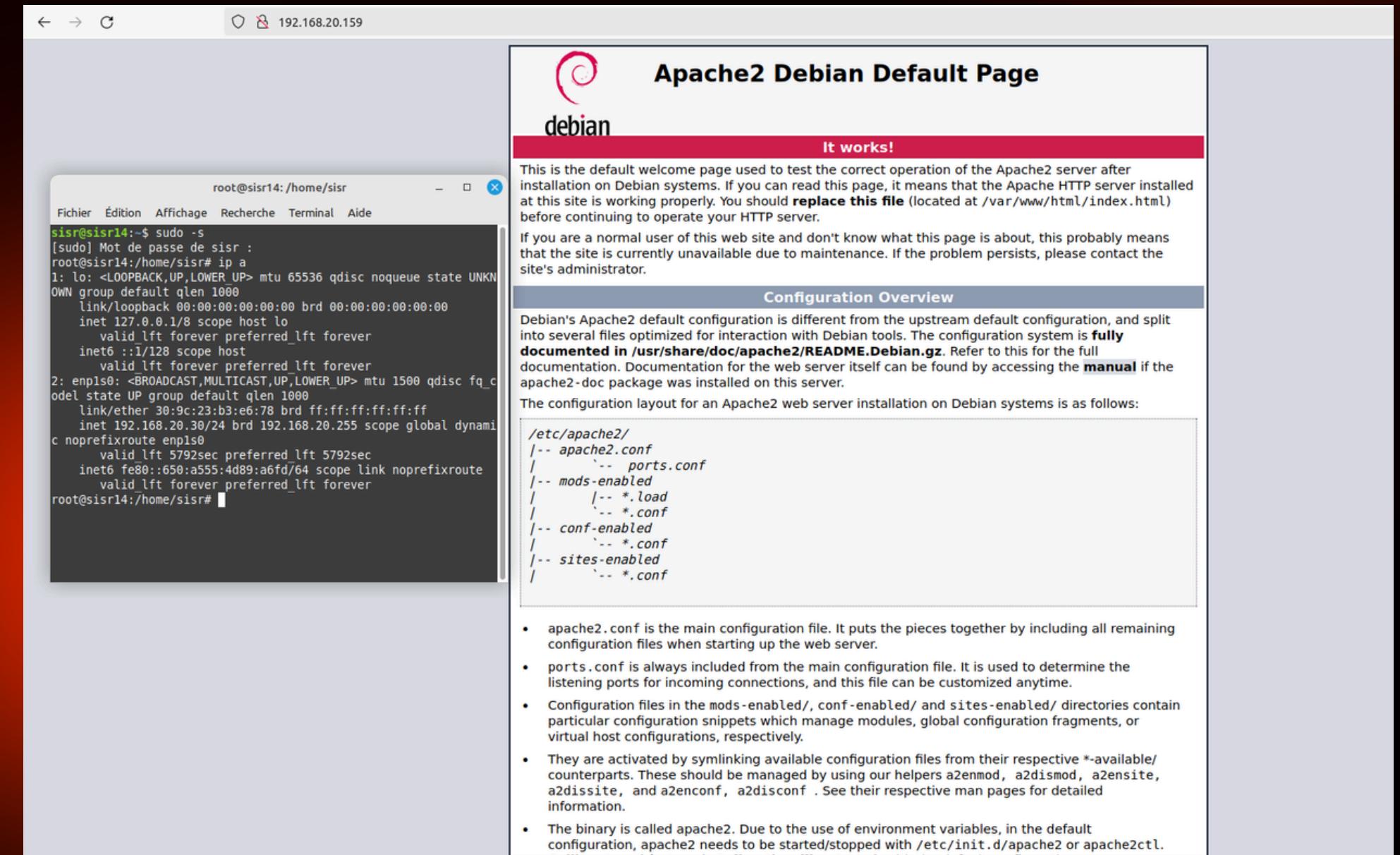
# WAN - TEST

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

The screenshot shows a 'Port Forward' configuration screen with the following data:

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
1	WAN	TCP	*	*	WAN address	50444	10.0.0.60	3389 (MS RDP)		
2	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.50	80 (HTTP)	Port forward HTTP vers lamp	

At the bottom, there are buttons for 'Add', 'Delete', 'Save', and 'Separator'.

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.

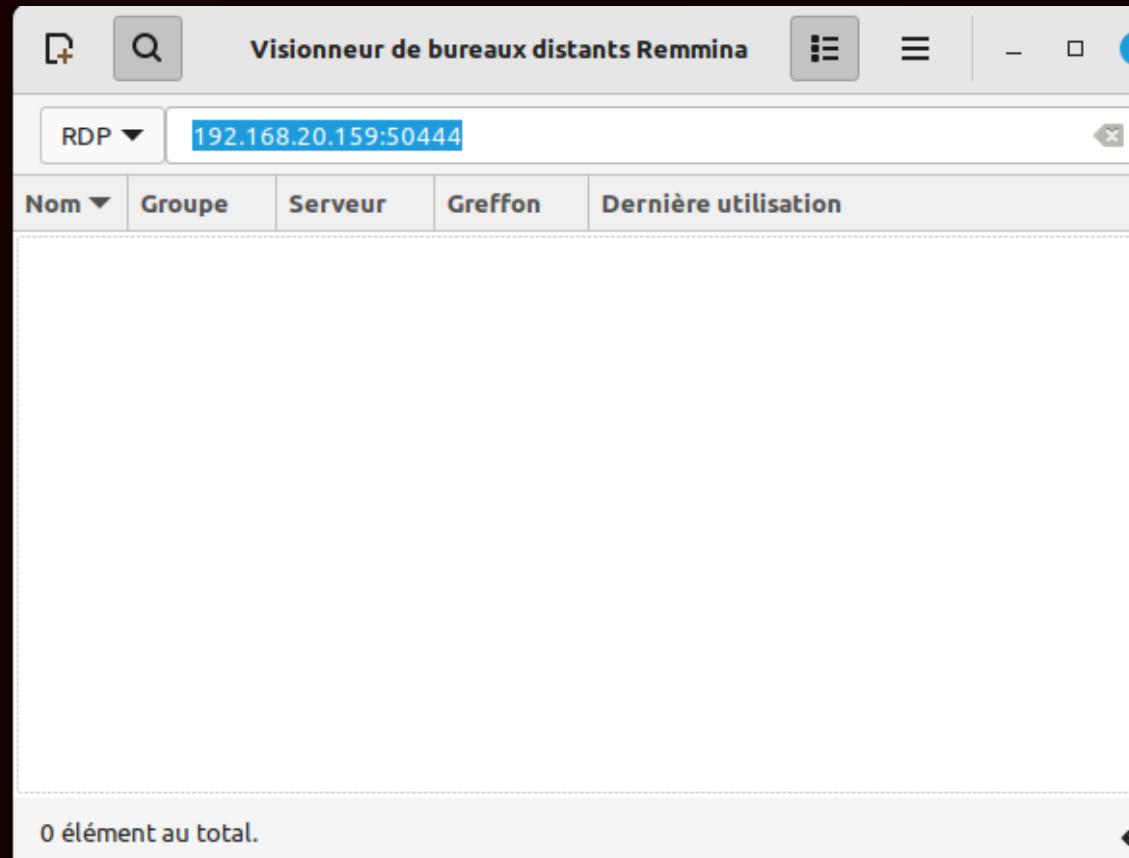
10.0.0.60 étant l'IP de mon serveur Windows situé dans la DMZ.

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.



01

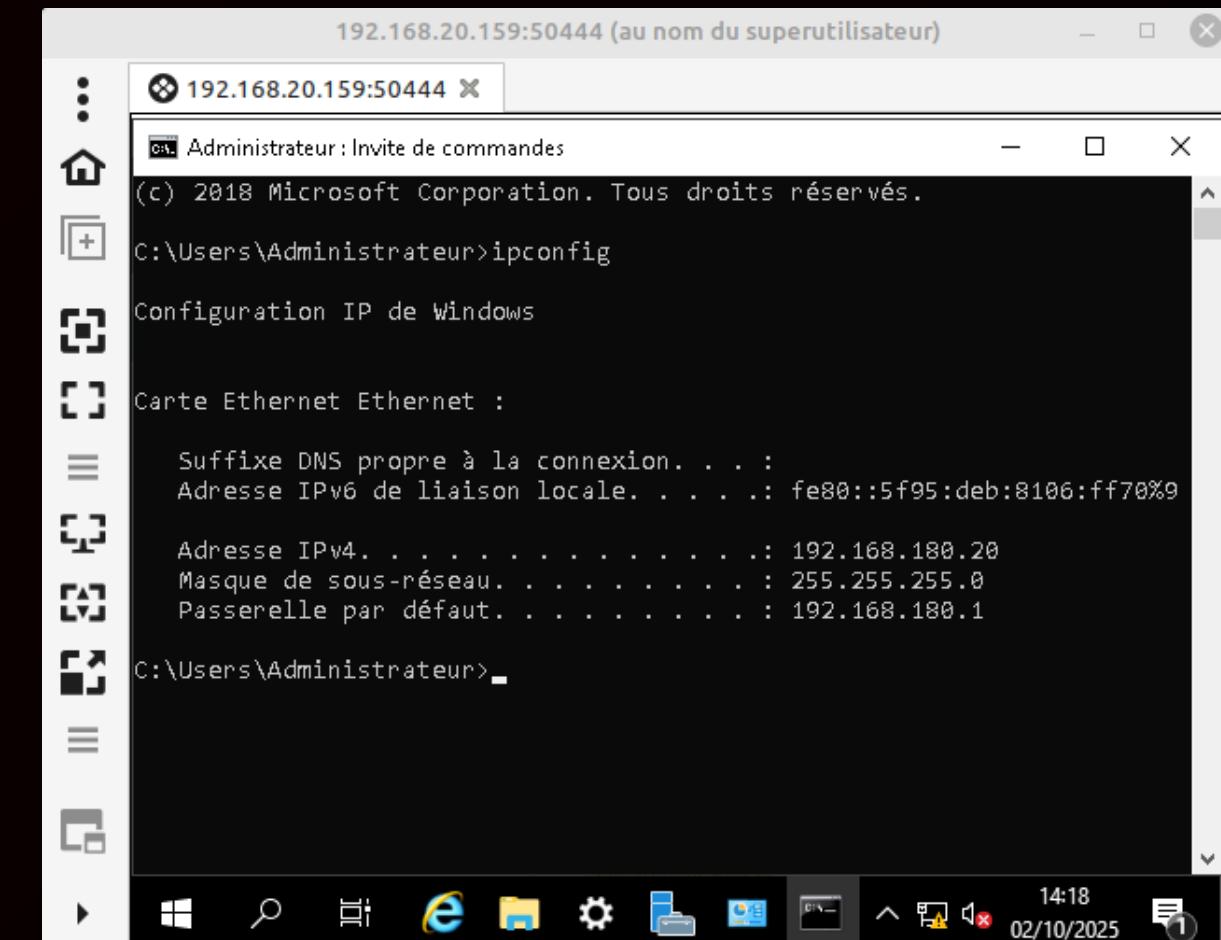
Avec Remmina, qui offre un accès au bureau à distance.



# RDP

0

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



# ZABBIX

01

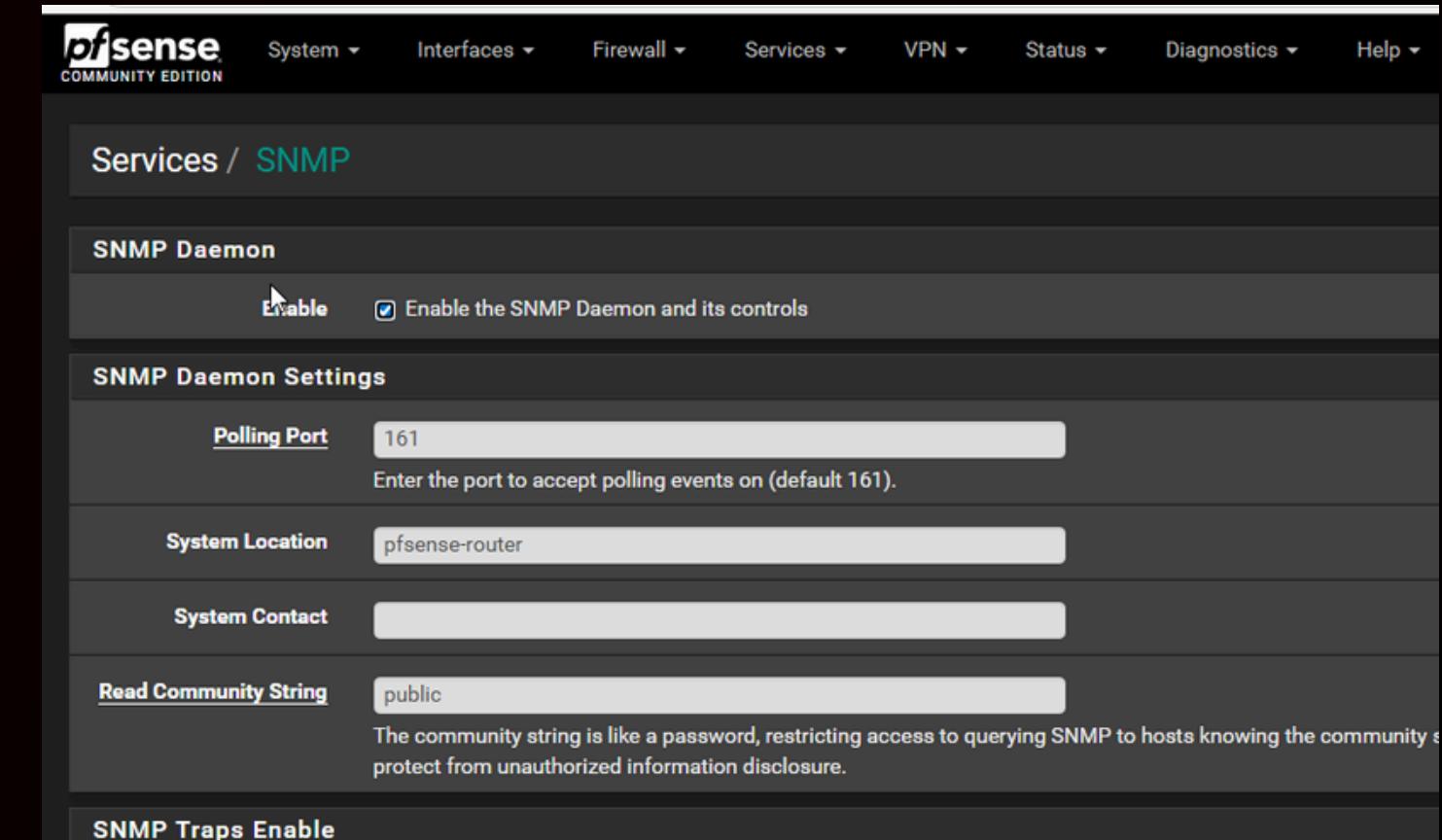
La solution choisie pour surveiller pfSense est Zabbix, car elle est facile à installer et fonctionne très bien avec ce système. Elle permet de surveiller en temps réel l'état du pare-feu, comme l'utilisation du processeur, de la mémoire ou du trafic réseau. Zabbix peut également envoyer des alertes 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.

**Hôte**

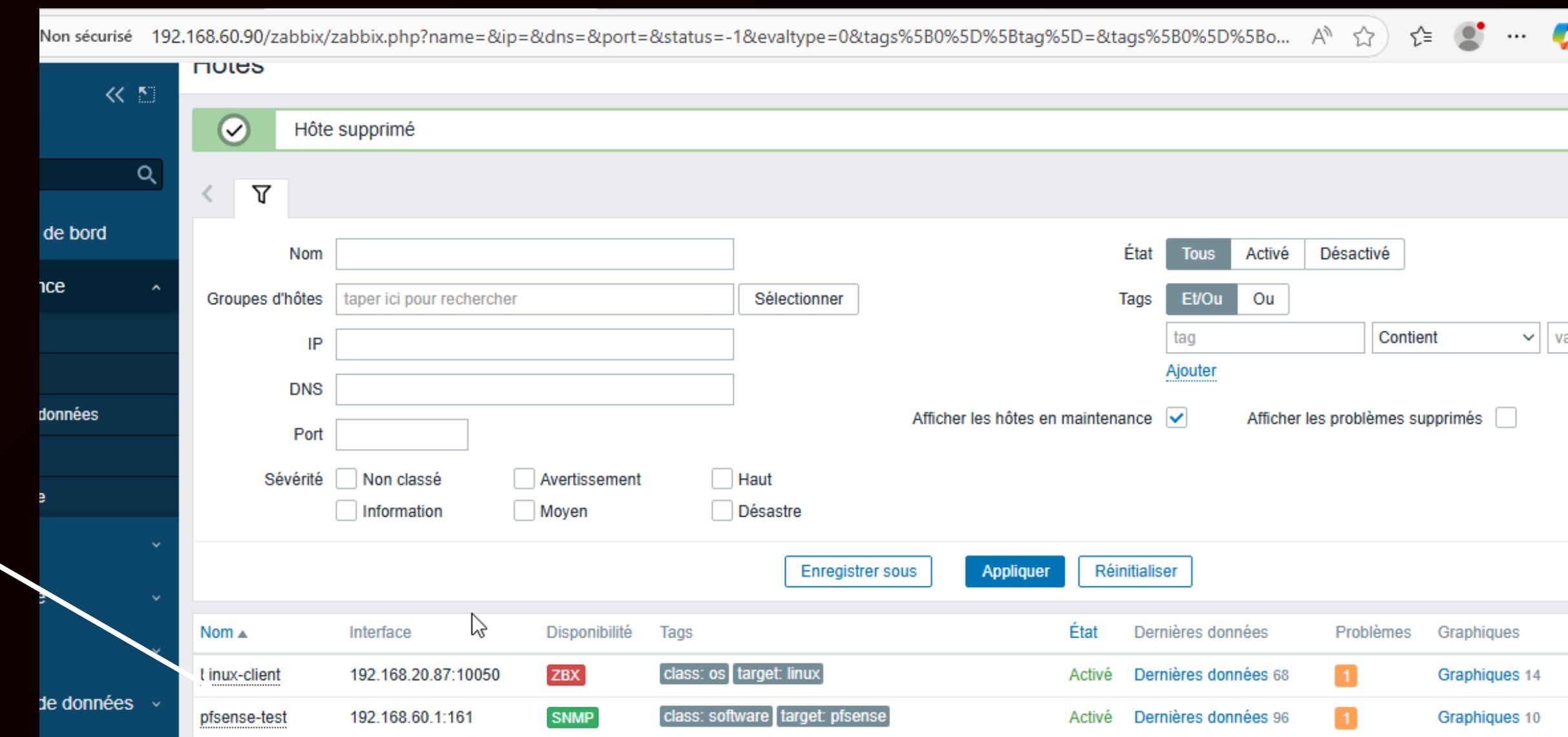
Hôte	IPMI	Tags	Macros	1	Inventaire	Chiffrement	Table de correspondance
* Nom de l'hôte	pfSense-test						
Nom visible	pfSense-test						
Modèles	Nom	Action					
	PFSense by SNMP	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>					
	taper ici pour rechercher	<a href="#">Sélectionner</a>					
* Groupes d'hôtes	Virtual machines	<a href="#">Sélectionner</a>					
	taper ici pour rechercher						
Interfaces	Type	adresse IP	Nom DNS			Connexion à	Port
	SNMP	192.168.60.1				<a href="#">IP</a>	<a href="#">DNS</a>
						<a href="#">161</a>	

**Modèles**

Nom	Action
PFSense by SNMP	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>
Agent	
Plus de correspondances trouvées...	
Linux by Zabbix agent	
FreeBSD by Zabbix agent	

# ZABBIX - RESULTAT

Et mon PFSense est bien remonté



The screenshot shows the Zabbix web interface at the URL [192.168.60.90/zabbix/zabbix.php?name=&ip=&dns=&port=&status=-1&evaltype=0&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5B0%5D](http://192.168.60.90/zabbix/zabbix.php?name=&ip=&dns=&port=&status=-1&evaltype=0&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5B0%5D). A note at the top says "Hôte supprimé" (Host deleted). The host list table shows two hosts:

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques
linux-client	192.168.20.87:10050	ZBX	class: os   target: linux	Activé	Dernières données 68	1	Graphiques 14
pfsense-test	192.168.60.1:161	SNMP	class: software   target: pfsense	Activé	Dernières données 96	1	Graphiques 10