



PFSENSE

F I R E W A L L



SOMMAIRE

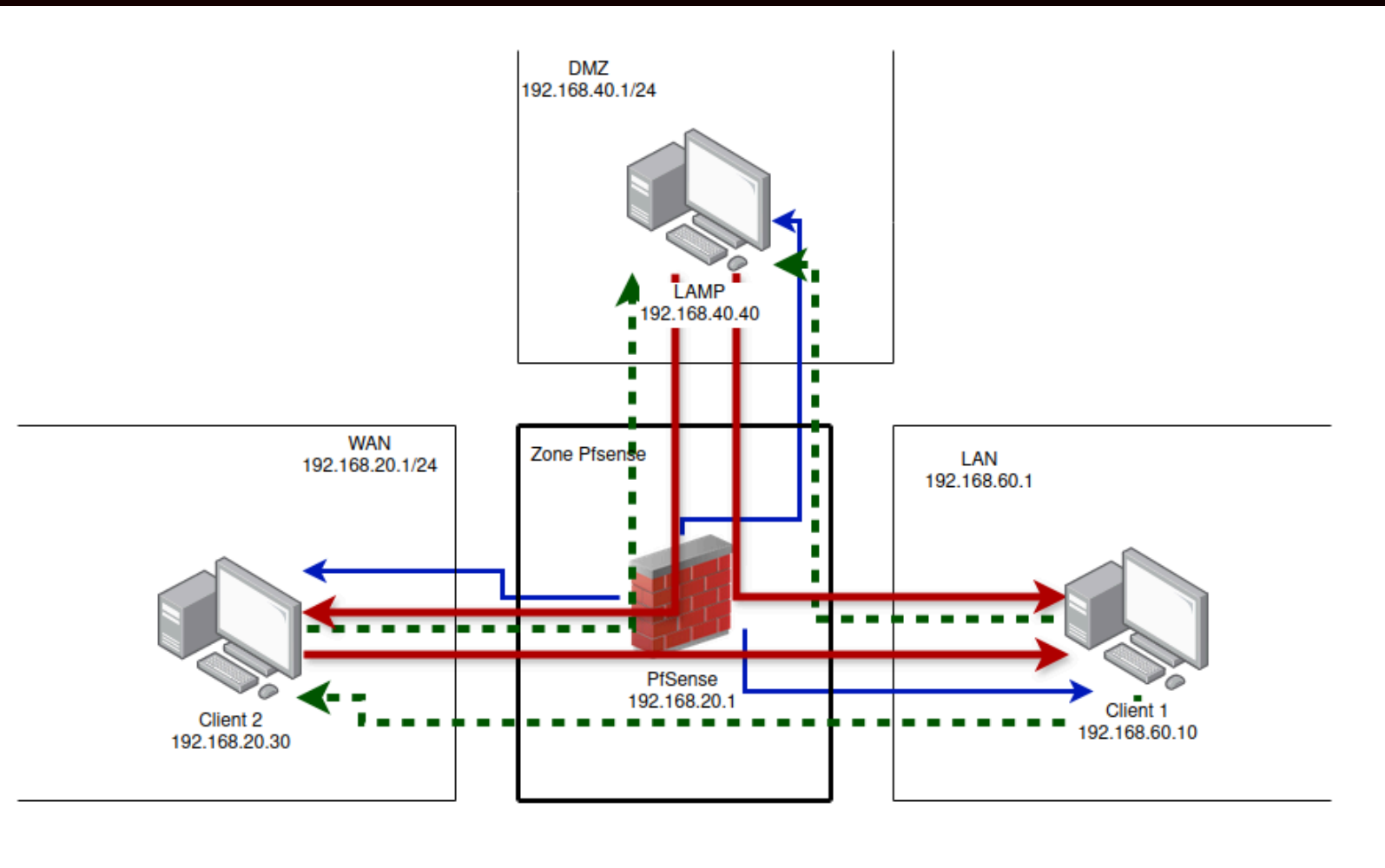
- QU'EST CE QUE PFSENSE
- INSTALLATION
- INTERFACE PFSENSE
- REGLE NAT
- DMZ - TEST
- LAN - TEST
- WAN - TEST
- RDP ET REGLE NAT
- ZABBIX
- ZABBIX - RESULTAT



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

```
mon quest - netgate device id: 010210012300031031010
*** 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

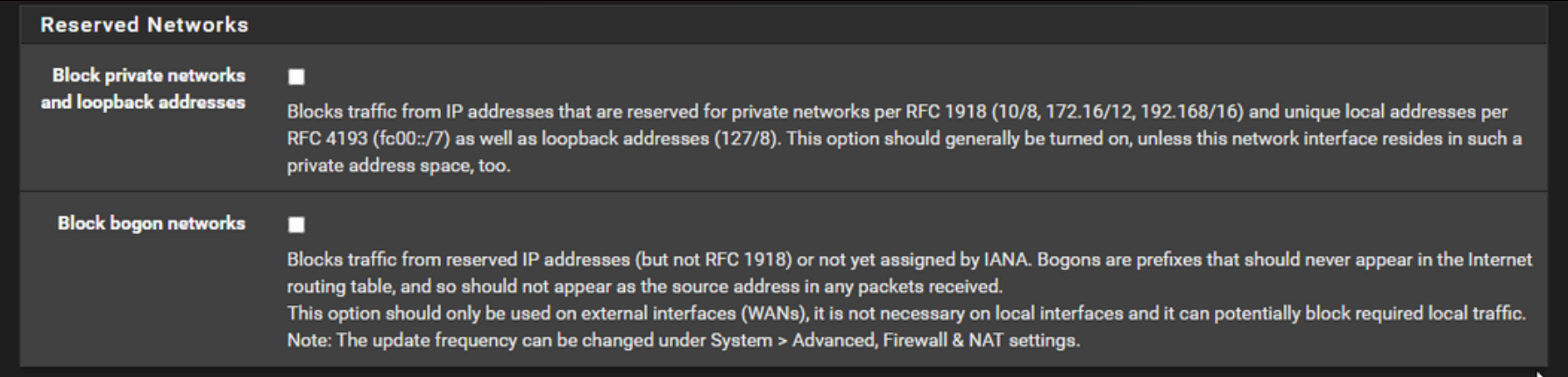
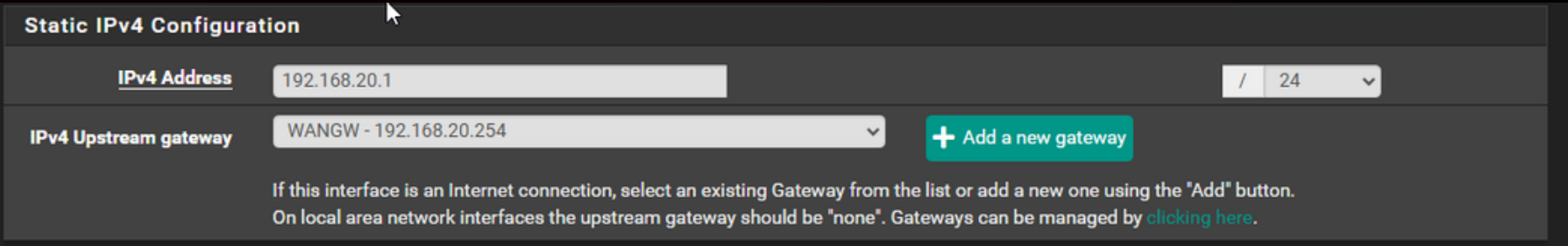
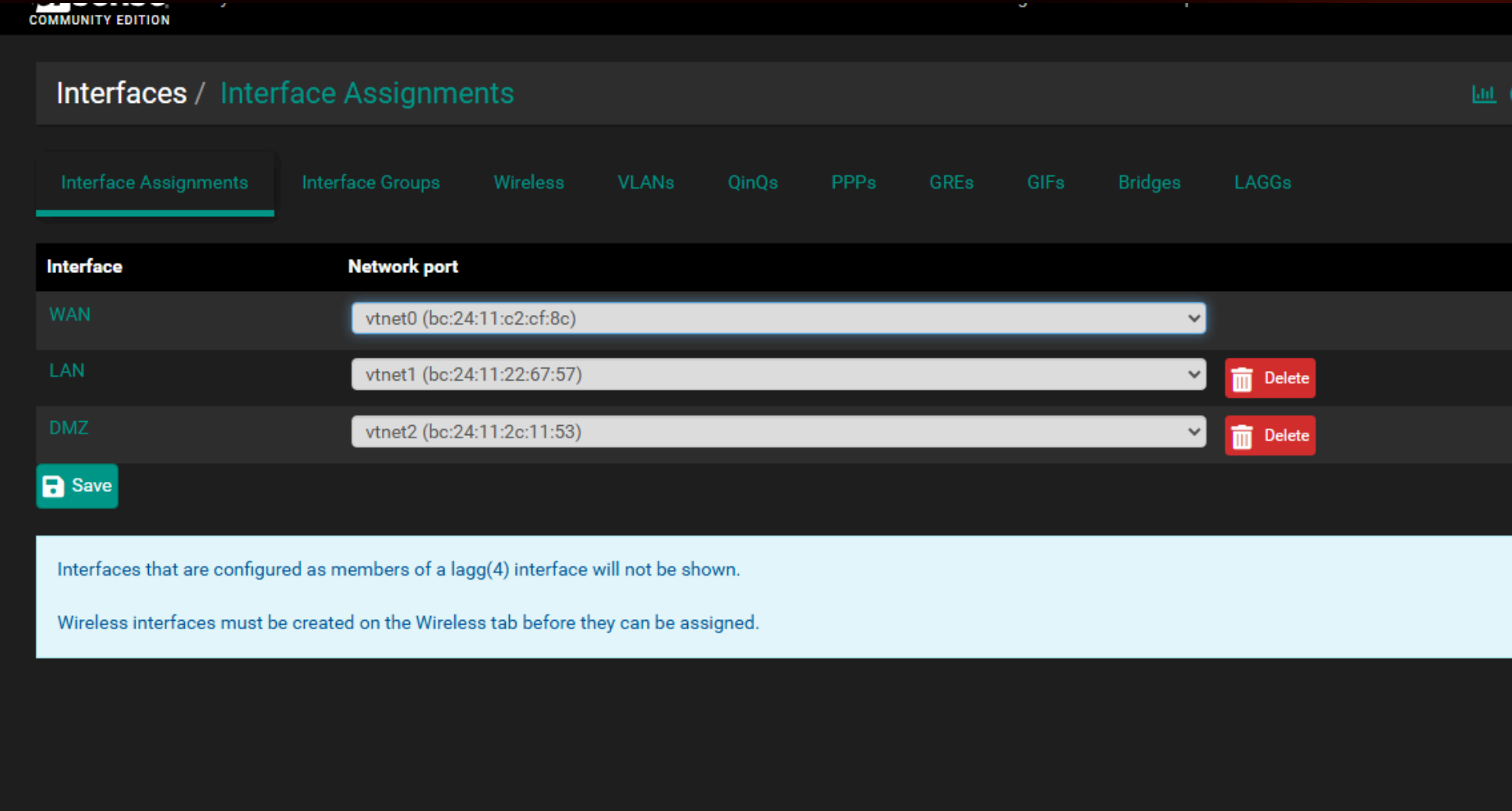
En local, saisissez l'adresse IP de votre pfSense (192.168.20.1) et vous arriverez sur une interface graphique (identifiant = admin, mot de passe = mdp VMpfsense).

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.





REGLE NAT

01

Firewall / NAT / Port Forward / Edit

Port Forward 1:1 Outbound NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	50444	10.0.0.60	3389 (MS RDP)		
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.50	80 (HTTP)	Port forward HTTP vers lamp	

Add Add Delete Save Separator

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.
```




Accès du LAN a LA DMZ

← ↻ ⚠ Non sécurisé 10.0.0.50



Apache2 Debian

This is the default welcome page used to test the installation on Debian systems. If you can see this page, the installation at this site is working properly. You can find more information about the Debian web server at <http://www.debian.org/webserver/> before continuing.

If you are a normal user of this web site and you are having problems, you should first check that the site is currently unavailable due to a temporary problem with the site's administrator.

Configuration

Debian's Apache2 default configuration is different from the default configuration of other operating systems. It is documented in **/usr/share/doc/apache2-doc** package. Documentation for the web server is available in the **apache2-doc** package was installed on this system.

The configuration layout for an Apache2 web server on Debian is as follows:

```
/etc/apache2/
|-- apache2.conf
/   |-- ports.conf
|-- mods-enabled
/   |-- *.load
/   |-- *.conf
|-- conf-enabled
/   |-- *.conf
|-- sites-enabled
/   |-- *.conf
```

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

invite de commandes

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
Réponse de 192.168.20.159 : octets=32 temps<1ms TTL=64
Réponse de 192.168.20.159 : octets=32 temps<1ms TTL=64
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 :

Suffixe 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>

LAN - TEST

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

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



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.
```

← → ↺ 192.168.20.159

root@sisr14: /home/sisr

Fichier Édition Affichage Recherche Terminal Aide

```
sisr@sisr14:~$ sudo -s
[sudo] Mot de passe de sisr :
root@sisr14:/home/sisr# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 30:9c:23:b3:e6:78 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.30/24 brd 192.168.20.255 scope global dynamic noprefixroute enp1s0
        valid lft 5792sec preferred_lft 5792sec
    inet6 fe80::650:a555:4d89:a6fd/64 scope link noprefixroute
        valid lft forever preferred_lft forever
root@sisr14:/home/sisr#
```

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`.

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.

LUCA BONA

09



RDP ET REGLE NAT

01

Firewall / NAT / Port Forward / Edit

Port Forward 1:1 Outbound NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	50444	10.0.0.60	3389 (MS RDP)		
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.50	80 (HTTP)	Port forward HTTP vers lamp	

Add Add Delete Save 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.

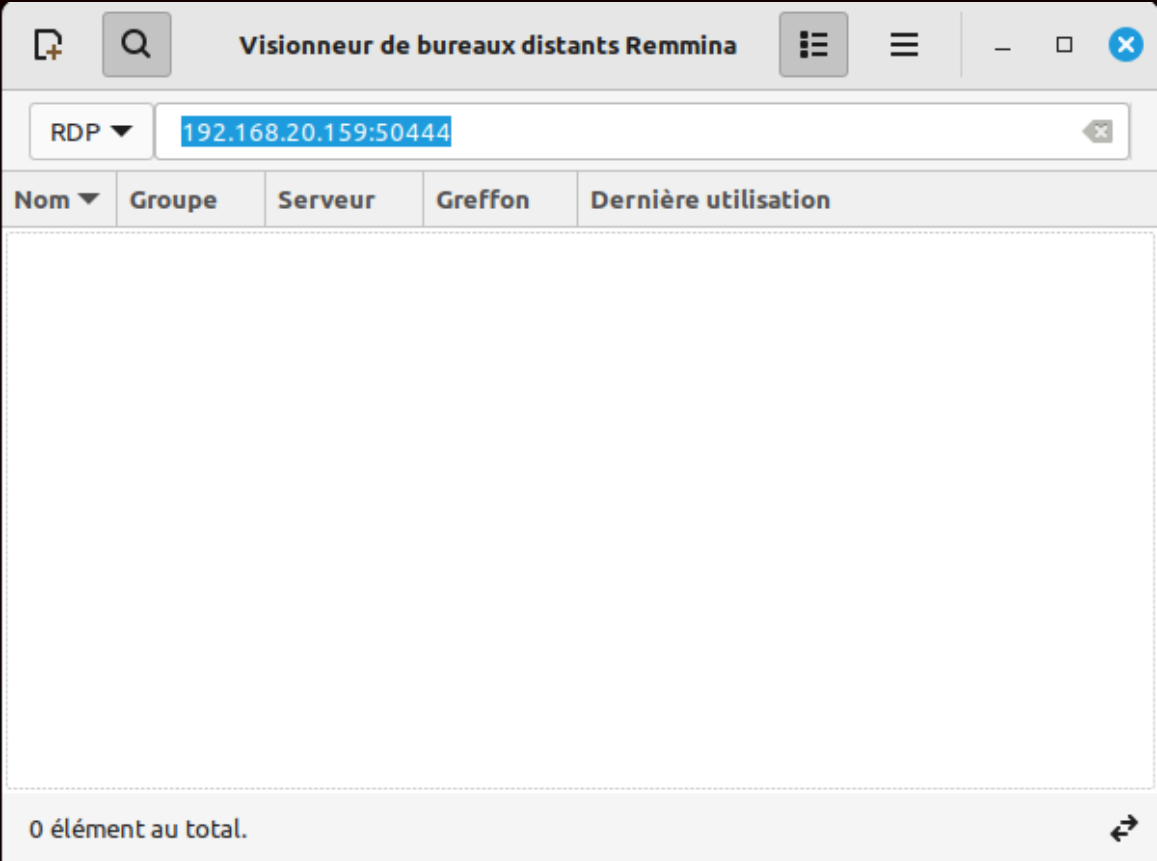
Le port de destination est "50444", mais j'aurais pu mettre "49054" ou "83904", peu importe, car le port RDP par défaut est le 3389 et l'utiliser tel quel peut représenter une faille de sécurité.

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



01

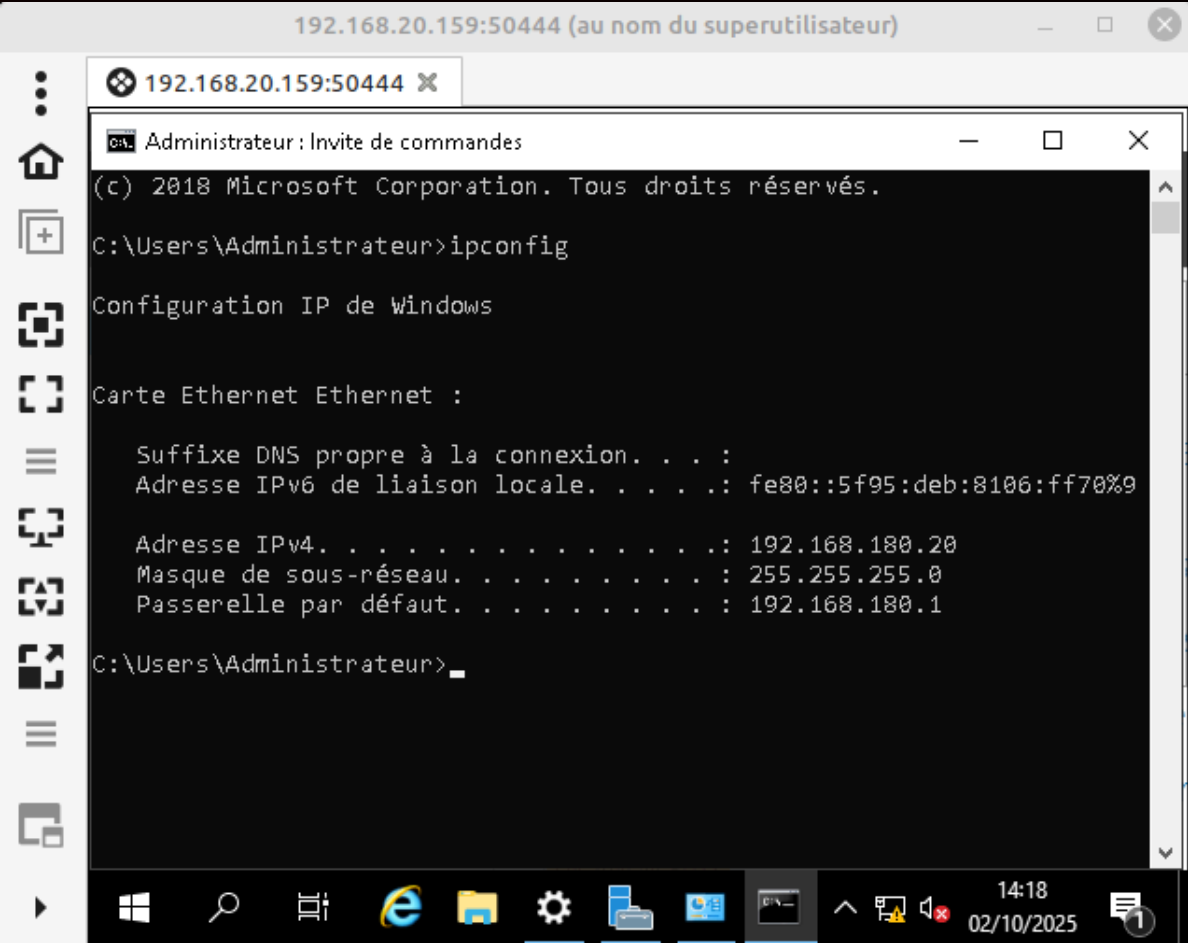
Avec Remmina, qui offre un accès au bureau à distance.



RDP

02

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





ZABBIX

01

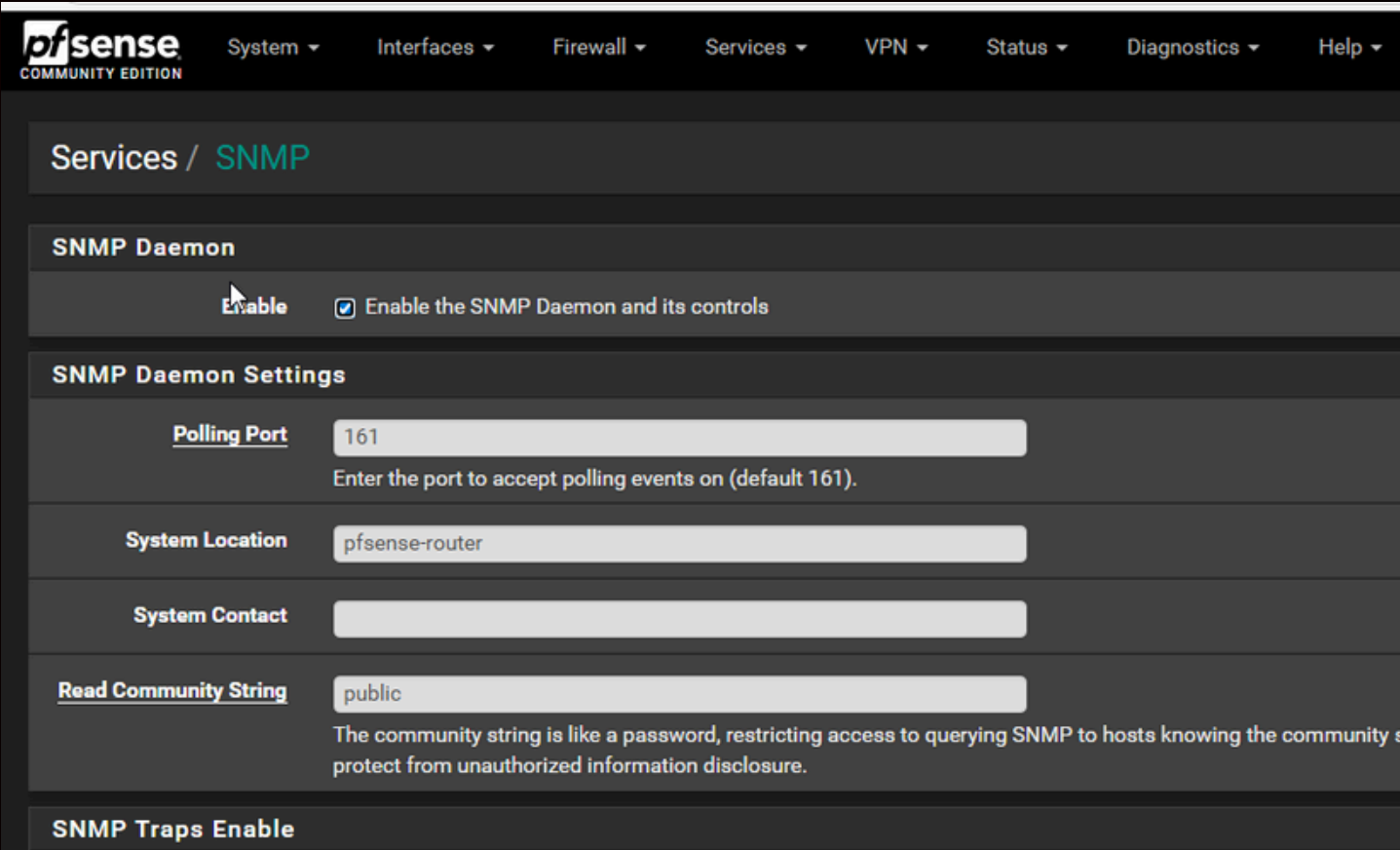
La solution choisie pour surveiller pfSense est Zabbix, car elle est facile à installer et fonctionne très bien avec ce système. Elle permet de surveiller en temps réel l'état du pare-feu, comme l'utilisation du processeur, de la mémoire ou du trafic réseau. Zabbix peut également envoyer des alertes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

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.

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.





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.

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

[Supprimer lien](#)

[Supprimer lien et nettoyer](#)

taper ici pour rechercher

Sélectionner

* Groupes d'hôtes

Virtual machines

taper ici pour rechercher

Sélectionner

Interfaces

Type

adresse IP

Nom DNS

Connexion à

Port

▼ SNMP

192.168.60.1

IP

DNS

161

Modèles

Nom

Action

PFSense by SNMP

[Supprimer lien](#)

[Supprimer lien et nettoyer](#)

Agent

Plus de correspondances trouvées...

Linux by Zabbix agent

FreeBSD by Zabbix agent



ZABBIX - RESULTAT

Et mon PFSense est bien remonté

Non sécurisé 192.168.60.90/zabbix/zabbix.php?name=&ip=&dns=&port=&status=-1&evaltype=0&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5Bo...

notes

✓ Hôte supprimé

< [Filter Icon]

Nom

Groupes d'hôtes Sélectionner

IP

DNS

Port

État

Tags

Contient

Afficher les hôtes en maintenance ☒ Afficher les problèmes supprimés ☐

Sévérité ☐ Non classé ☐ Avertissement ☐ Haut ☐ Information ☐ Moyen ☐ Désastre

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