Amine Boukherouba BTS SIO SISR

Compte-rendu

Contexte :

La société Amine nous a demandé d'intervenir afin de mettre en place un système de surveillance sur le réseau. Ce réseau contiendra un LAN avec un routeur.
Nous pourrons le configurer afin d'avoir plusieurs fonctionnalités comme laisser l'accès au SSH ou au RDP. Le système de surveillance est Zabbix et il va nous permettre de surveiller tous les appareils présents sur notre réseau.

Sommaire:

Prérequis :

- Un routeur Pfsense
- Serveur Ubuntu 22.04 LTS
- Serveur Windows 2019

Explication :

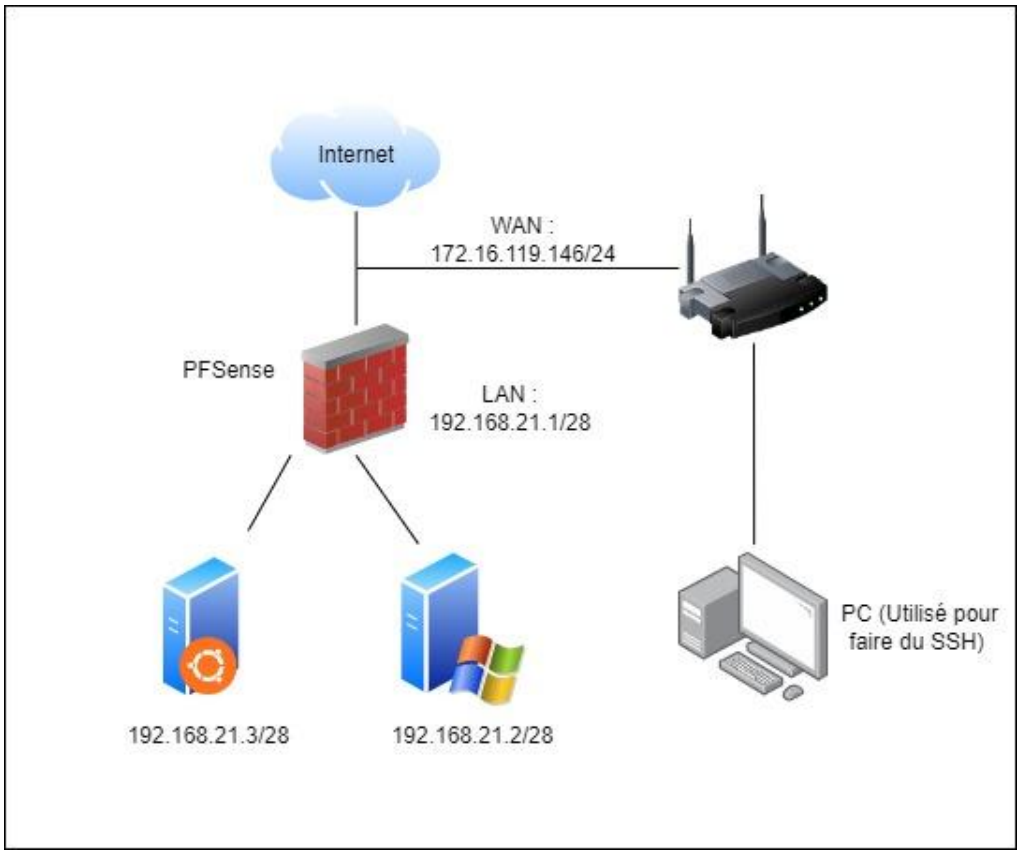
Tout d'abord, nous allons installer Zabbix sur un serveur Ubuntu en version 22.04.

Ensuite, nous allons installer Windows 2019 pour un serveur avec une configuration de la carte réseau.

Puis, on installera un routeur PFsense avec une configuration pour le sous-réseaux et la création d'une règle pour laisser passer le SSH si jamais on veut configurer le serveur Ubuntu.

Enfin, nous allons configurer Zabbix avec la possibilité d'ajouter des fonctionnalités pour être alerté lorsqu'il y a un problème sur le réseau.

Schéma de la mission :



Tutoriel :

1- Installation de Zabbix et configuration du serveur Windows 2019

```
serverlinux@serverlinux:~$ sudo apt-get install apache2 libapache2-mod-php maria
db-server php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql unzip cu
rl gnupg2 -y
```

Tout d'abord, on installe LAMP serveur pour le serveur HTTP.

```
serverlinux@serverlinux:~$ sudo nano /etc/php/8.1/apache2/php.ini
```

On configure le fichier configuration de php en changeant les paramètres pour notre serveur web.

```
memory_limit 256M
upload_max_filesize 16M
post_max_size 16M
max_execution_time 300
max_input_time 300
max_input_vars 10000
```

```
date.timezone = Europe/France
```

```
serverlinux@serverlinux:~$ systemctl restart apache2
```

On redémarre notre service apache2

```
serverlinux@serverlinux:~$ sudo mysql
```

On se connecte à la base de données MYSQL pour créer une base de données pour zabbix puis un utilisateur.

```
MariaDB [(none)]> CREATE DATABASE zabbixdb character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.004 sec)

MariaDB [(none)]> CREATE USER 'zabbixuser'@'localhost' IDENTIFIED BY 'password';

Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON zabbixdb.* TO 'zabbixuser'@'localhost'
 WITH GRANT OPTION;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> exit;
```

On vient d'accorder les privilèges à notre utilisateur "zabbixuser".

```
serverlinux@serverlinux:~$ sudo wget https://repo.zabbix.com/zabbix/6.2/ubuntu/p
ool/main/z/zabbix-release/zabbix-release_6.2-2%2Bubuntu22.04_all.deb
```

```
serverlinux@serverlinux:~$ sudo dpkg -i zabbix-release_6.2-2+ubuntu22.04_all.deb
```

```
serverlinux@serverlinux:~$ sudo apt update
```

On installe maintenant zabbix qui n'est disponible dans les repo d'ubuntu donc on l'installe à partir du site officiel.

```
serverlinux@serverlinux:~$ sudo apt install zabbix-server-mysql zabbix-frontend-
php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

On fait de même pour avoir Zabbix server.

```
serverlinux@serverlinux:~$ systemctl start zabbix-server
```

```
serverlinux@serverlinux:~$ systemctl enable zabbix-server
```

On active maintenant le serveur Zabbix.

```
serverlinux@serverlinux:~$ sudo nano /etc/zabbix/zabbix_server.conf
```

```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
```

On configure le fichier de configuration de zabbix serveur pour mettre un mot de passe à notre utilisateur.

```
serverlinux@serverlinux:~$ sudo systemctl restart zabbix-server zabbix-agent apa
che2
```

```
serverlinux@serverlinux:~$ systemctl enable zabbix-server zabbix-agent apache2
```

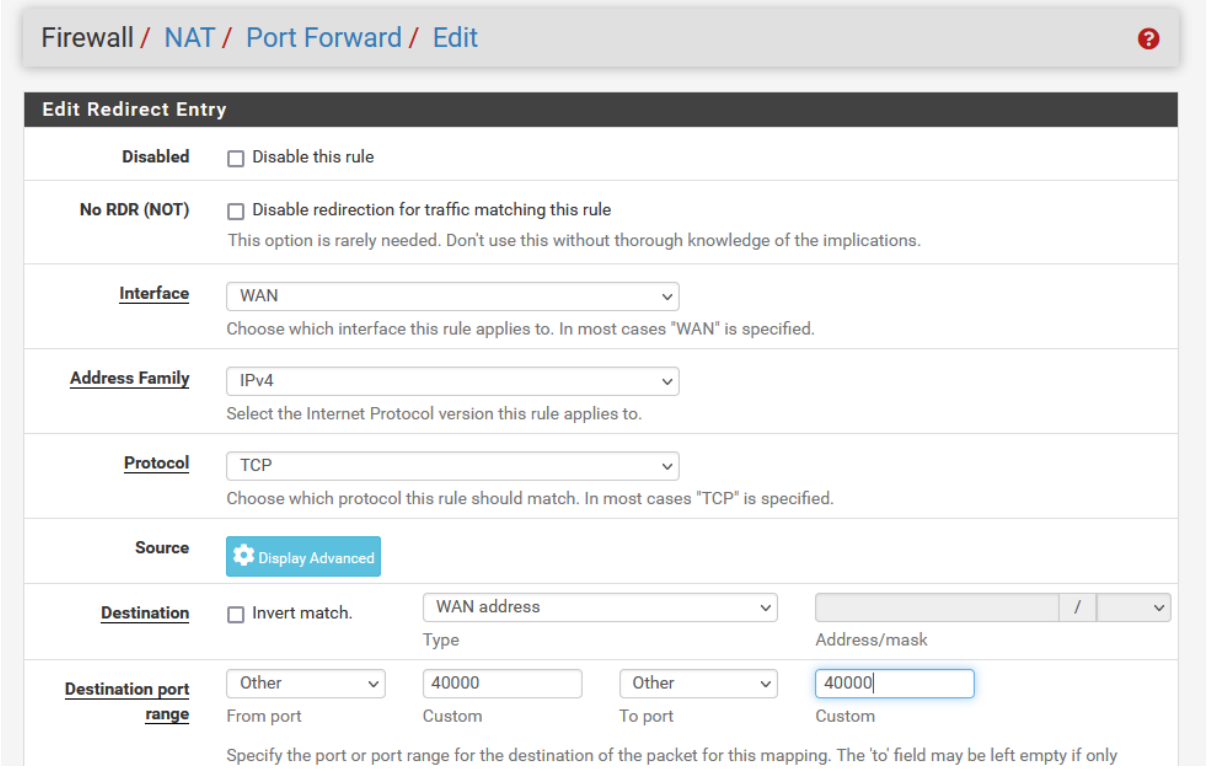
On active maintenant zabbix server.

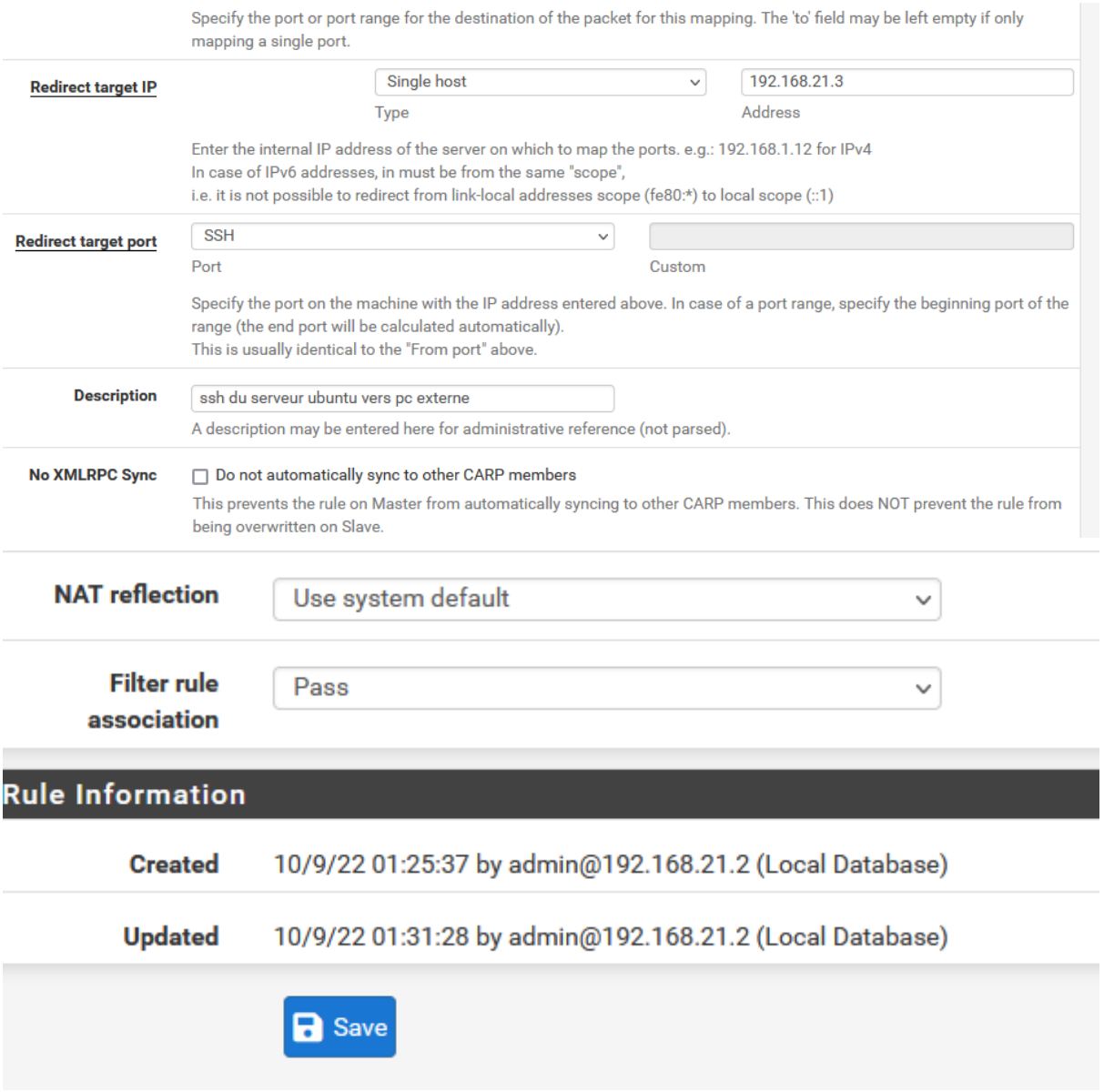
2- Configuration du routeur Pfsense,ubuntu serveur et Windows server 2019

```
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: dc74eef0bccd9054eb14

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

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.119.146/24
 LAN (lan)       -> em1        -> v4: 192.168.21.1/28

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: [zone: udp_inpcb] kern.ipc.maxsockets limit reached
arprequest: cannot find matching address
```

On sait qu'on à notre réseau en 192.168.21.0/28 donc on met notre pfsense sur notre première adresse.

SSH :





On crée une règle de redirection de port pour permettre l'accès depuis l'extérieur avec internet afin de se connecter en ssh avec un port personnalisé (pour une sécurité).

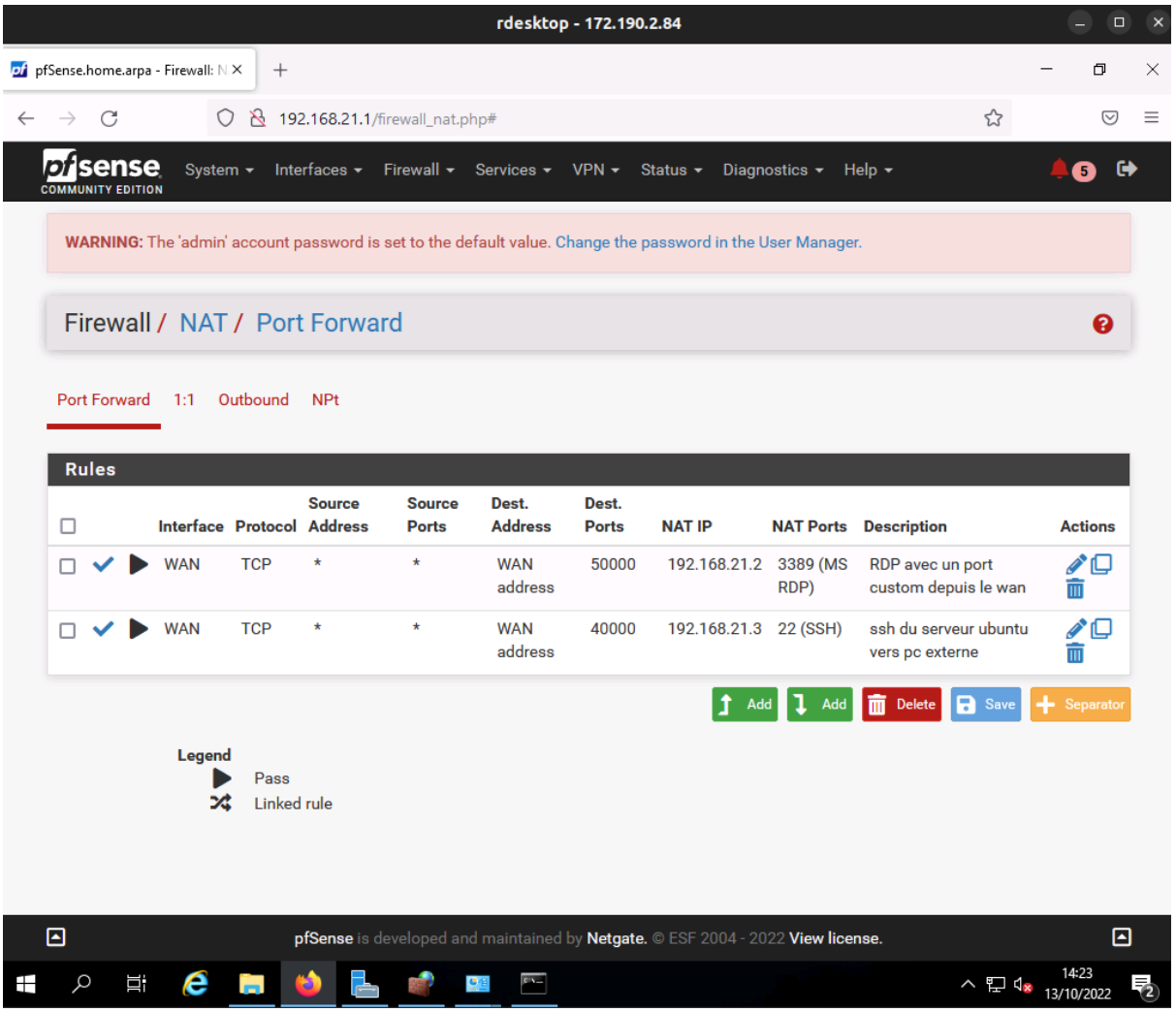
Le port par défaut du ssh est 22 mais on le customise en 40000.

Une requête envoyée sur l'adresse IP WAN du pfSense, sur le port 40000 sera automatiquement redirigée vers l'adresse IP 192.168.21.3 sur le port 22

```
amine@amine-Vector-GP66-12UGS:~$ ssh serverlinux@192.168.1.70 -p 40000
serverlinux@192.168.1.70's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of dim. 09 oct. 2022 01:41:21 UTC

  System load:  0.154296875       Processes:             280
  Usage of /:   47.9% of 13.67GB  Users logged in:       1
```

On remarque qu'on réussit bien à se connecter en SSH avec le port 40000 qui est redirigé.

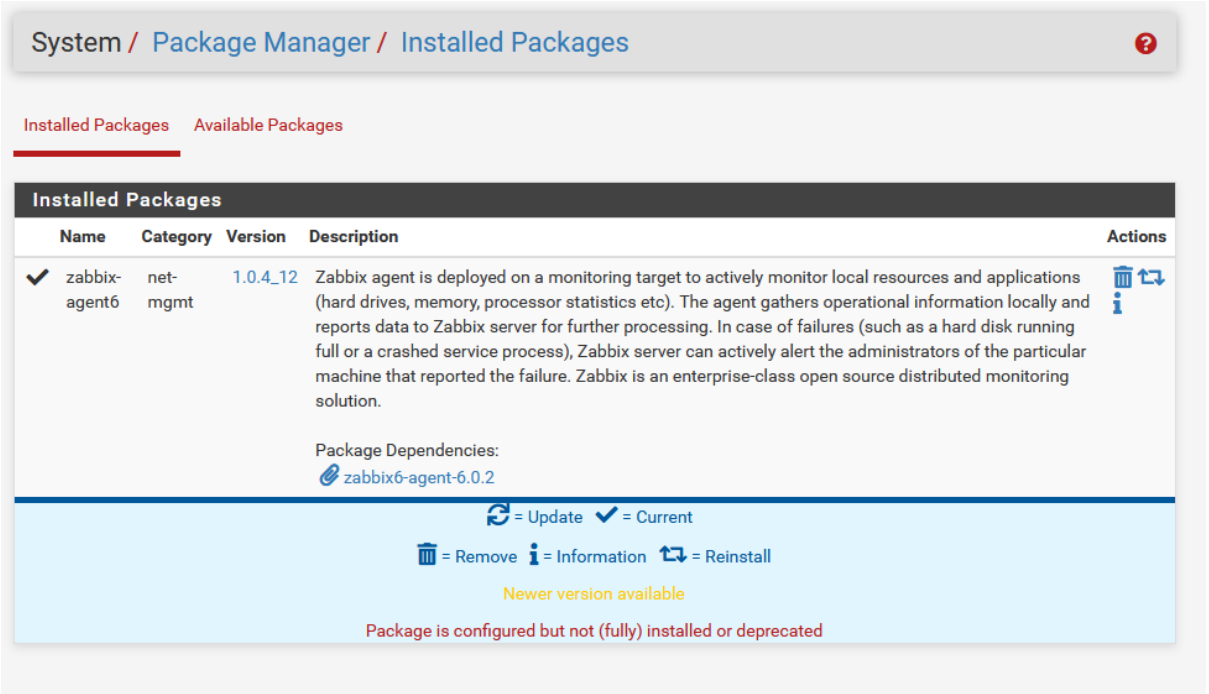
RDP :



On configure la redirection de port pour le RDP avec le port personnalisé en 50000 (on peut voir que je suis déjà connecté en RDP pour un test).

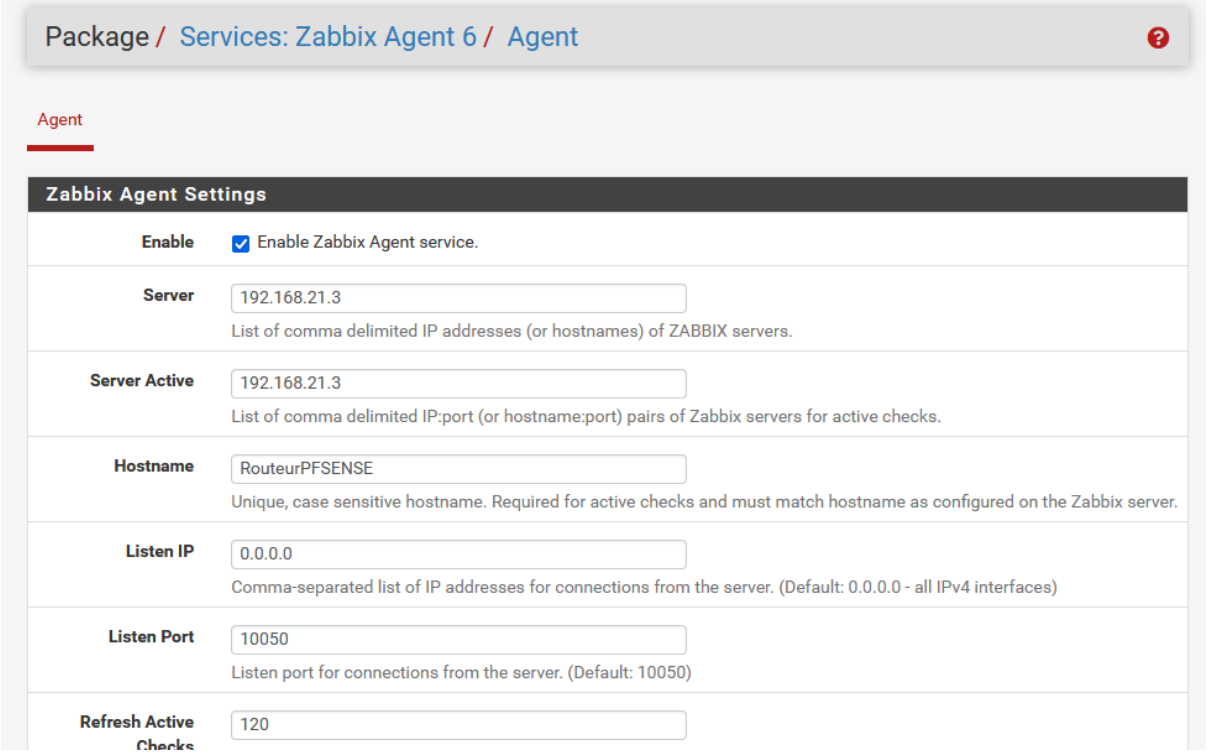
On installe rdesktop pour pouvoir accéder à distance à notre serveur Windows 2019, on rentre l'adresse ip de notre serveur et on met le port personnalisé qu'on a choisi.

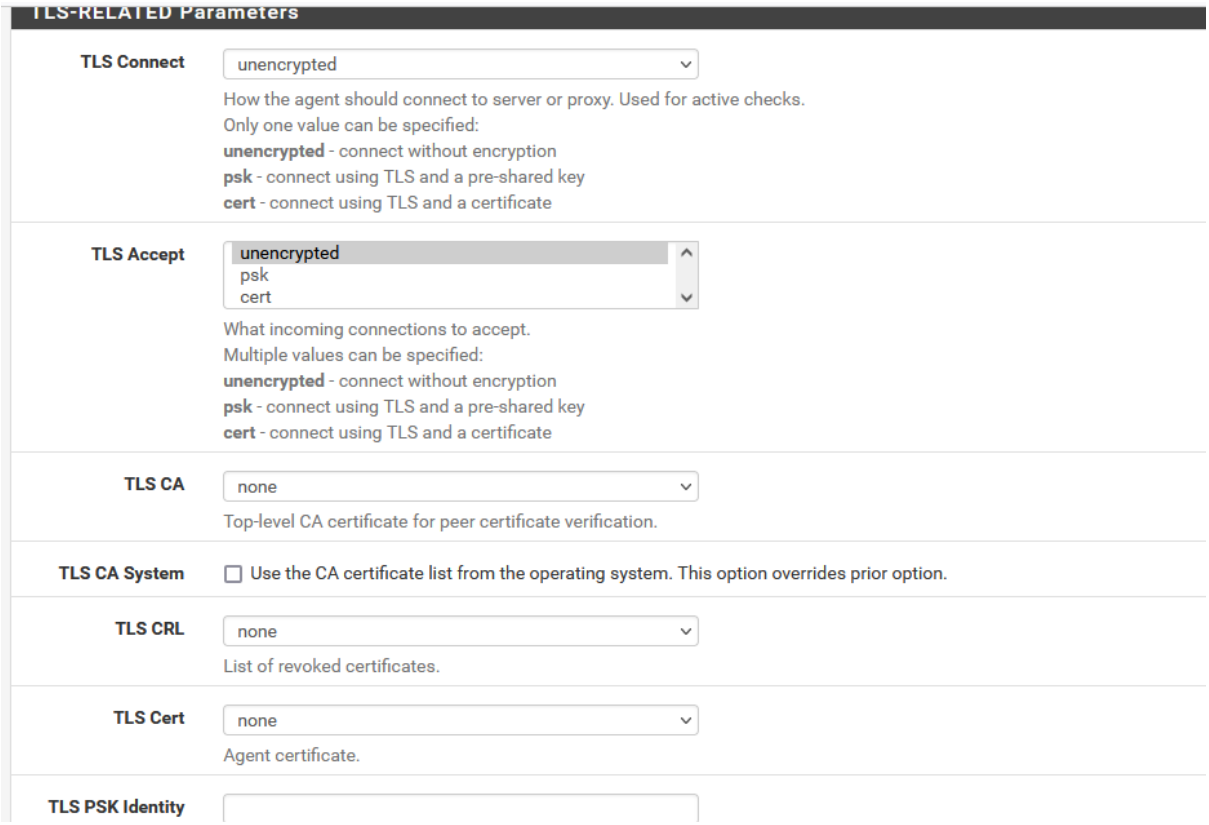
AGENT ZABBIX :



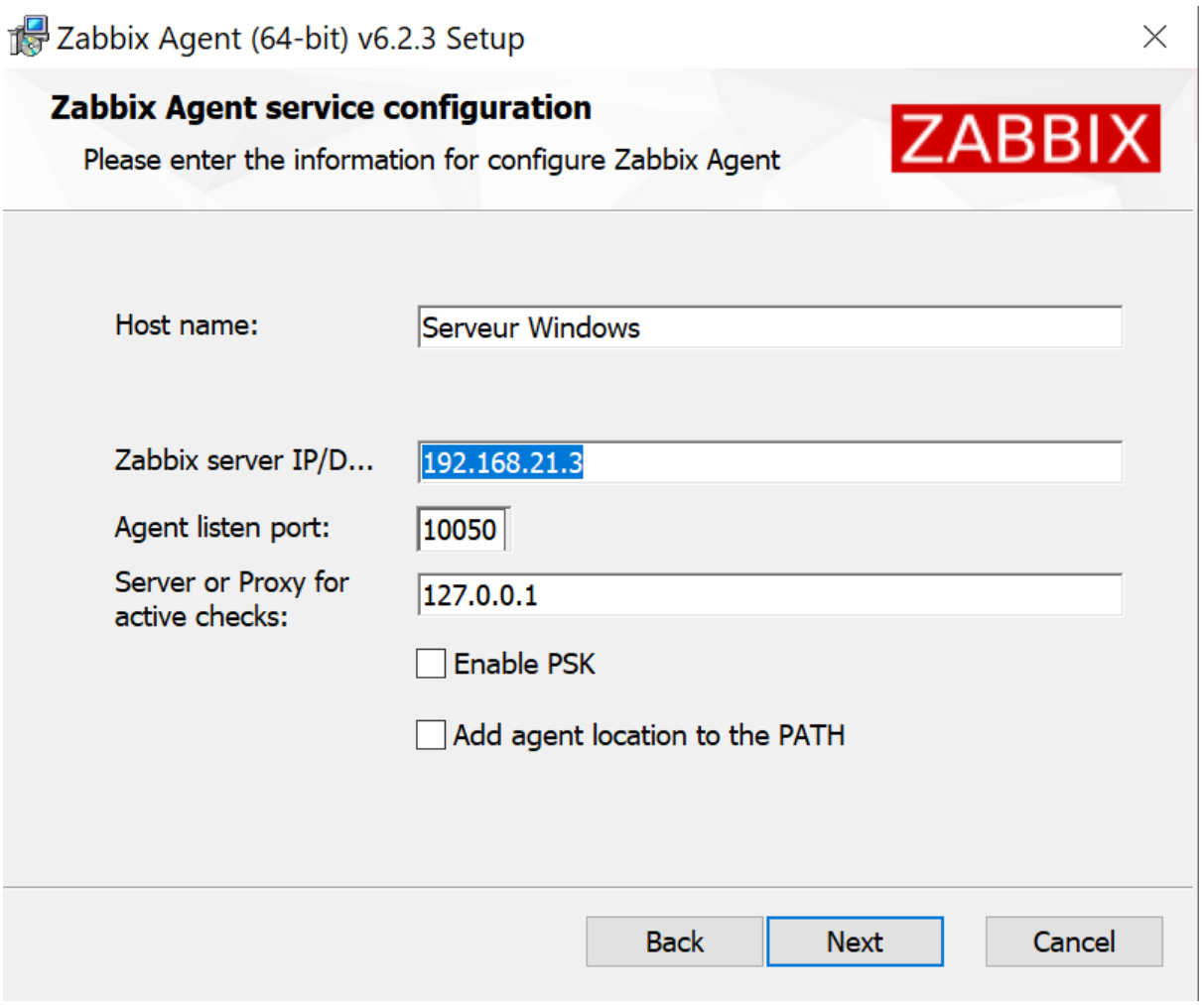
Amine Boukherouba BTS SIO SISR

On installe l'agent zabbix pour notre routeur pour qu'il remonte sur notre serveur zabbix.



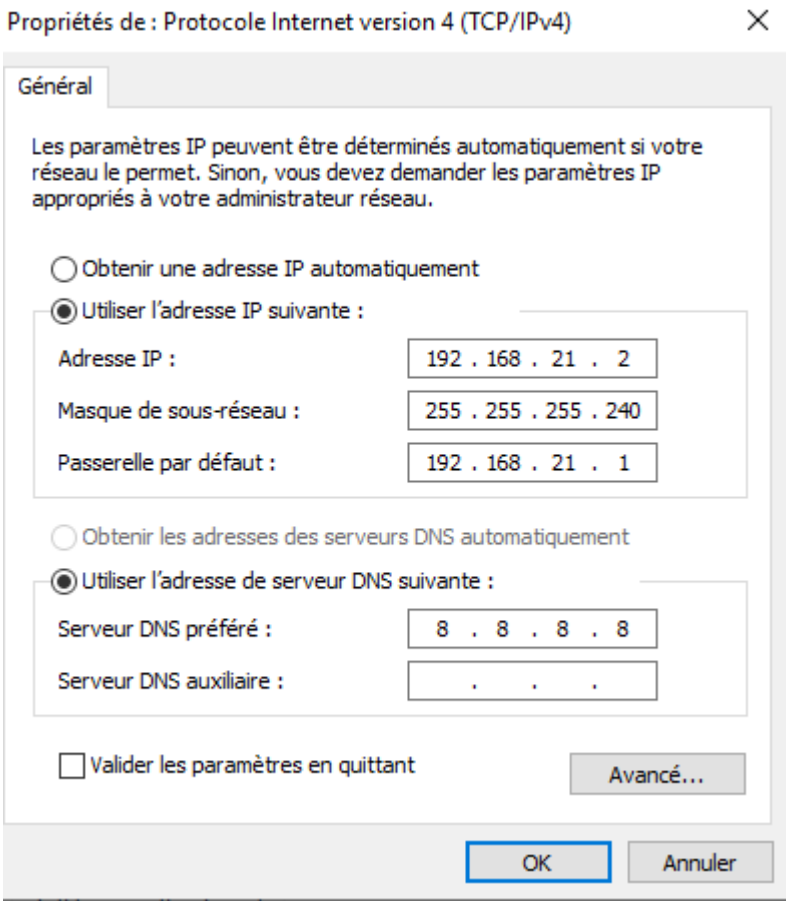


On active maintenant l'agent en renseignant l'ip de notre serveur zabbix.

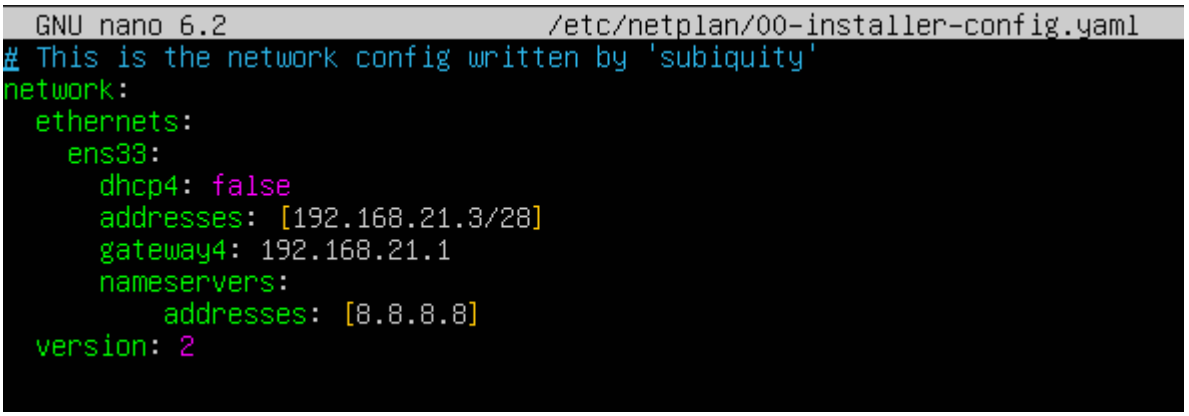


On fait de même sur notre serveur Windows.

CONFIGURATION IP :

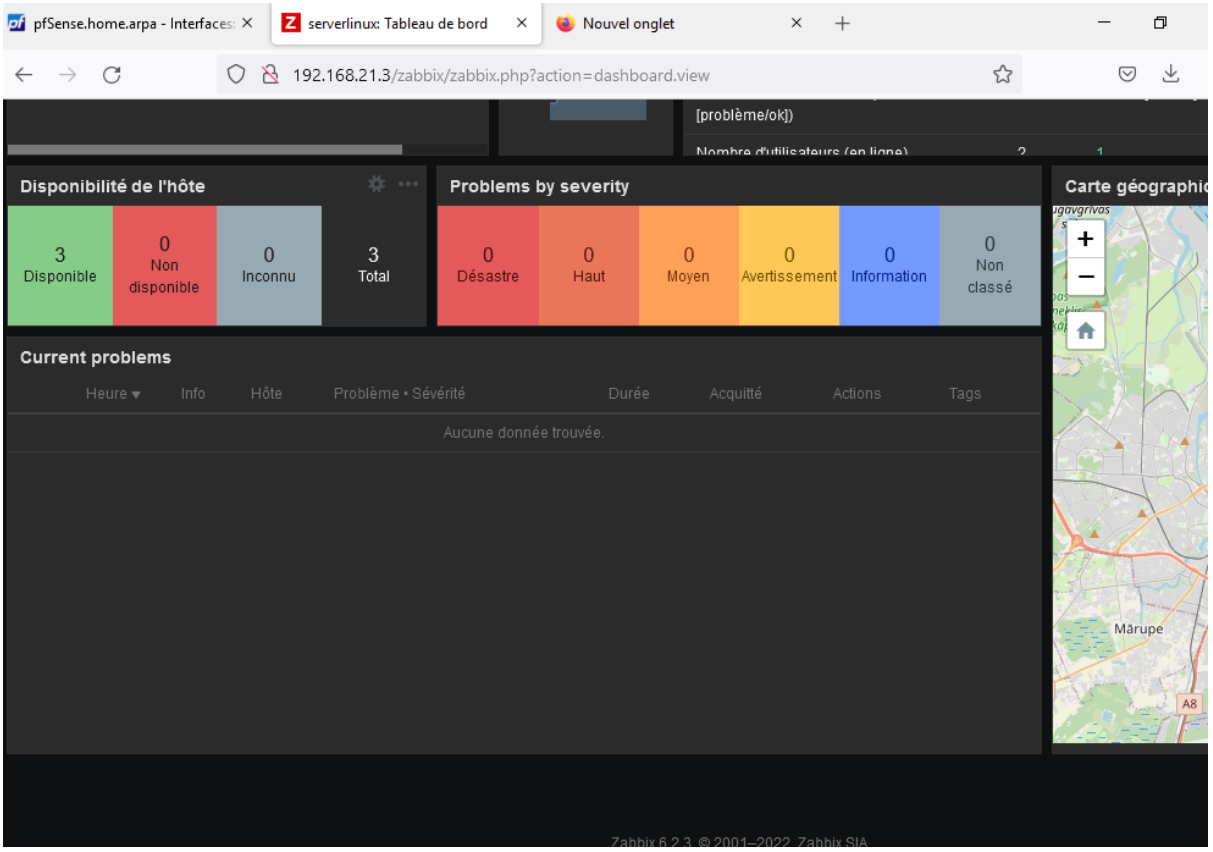


On met l'ip du serveur windows 2019 en 192.168.21.2/28 avec le routeur Pfsense en passerelle, notre DNS sera 8.8.8.8 pour avoir accès à internet.



On met ensuite notre Ubuntu server en 192.168.21.3/28 avec l'ip de notre PFsense en passerelle, notre DNS sera 8.8.8.8 pour avoir accès à internet.

3- Configuration de Zabbix



On ajoute nos trois hôtes donc le serveur Ubuntu qui contient Zabbix, notre serveur Windows 2019 et notre routeur PFSense (nos trois hôtes sont bien présent)

4- Test de la surveillance Zabbix

On vient de redémarrer le serveur PFsense pour tester si un problème va être détecté et remonter sur le serveur Zabbix et on remarque qu'il apparaît bien.

Conclusion :

On a bien rempli la mission qui est de mettre en place un système de monitoring (surveillance) sur notre réseau pour avoir des notifications et alertes en temps réel.
Ce réseau interne aura accès à internet.On pourra accéder à nos appareils à distance depuis l'extérieur grâce à des règles ssh qu'on a configurées sur notre routeur PFsense. Cela permettra de pouvoir gérer notre serveur Ubuntu. Bien évidemment, il faut ajouter tous les hôtes pour pouvoir recevoir des alertes et vérifier s' il y a des problèmes critiques (grâce à notre tableau de bord configurable).