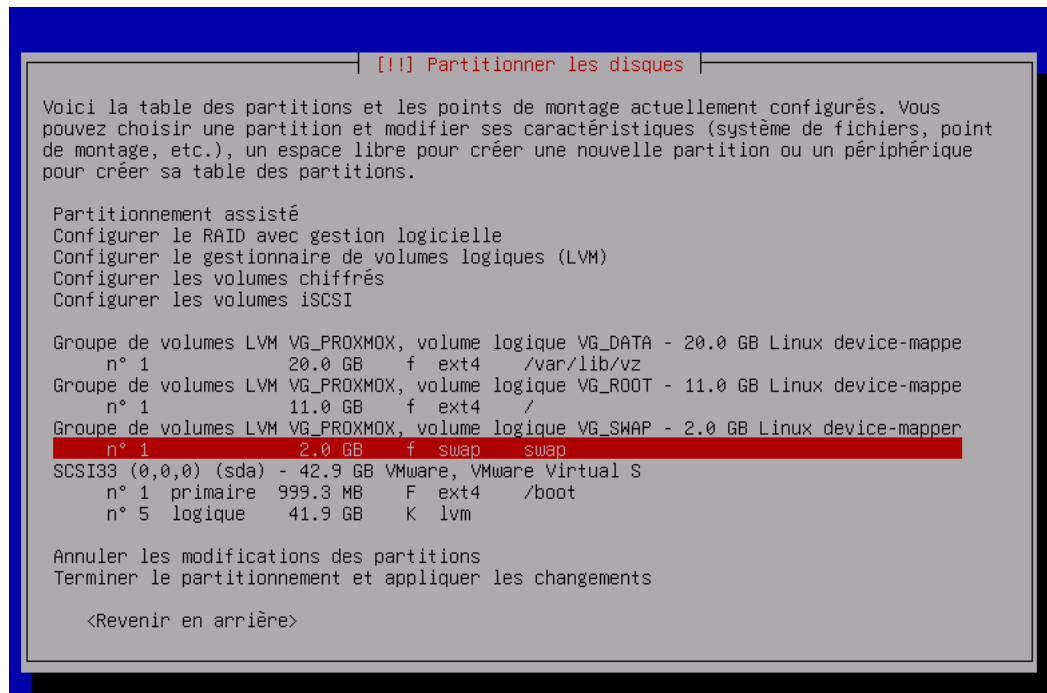


## Mise en place de Proxmox :

Dans un premier temps j'ai installé proxmox-pve sur une machine debian 12 afin de pouvoir utiliser cet hyperviseur, pour le partitionnement j'ai mis en place ce partitionnement il permettra d'avoir beaucoup de stockage pour pouvoir ajouter d'autres fonctionnalités pour une utilisation personnelle afin d'améliorer cette infrastructure au maximum :



```
root@debian:~# lsblk -f
NAME        FSTYPE     FSVER     LABEL  UUID                                  FSAVAIL FSUSE% MOUNTPOINTS
loop0       ext4        1.0       loop0  21238312-0928-4918-80bb-bc8aad353471
loop1       ext4        1.0       loop1  5bd34221-2e62-4d54-b618-4f6a5f865831
loop2       ext4        1.0       loop2  58fcb8bb-ecab-477e-bbb6-f662e3027d22
loop3       ext4        1.0       loop3  41438554-2cf5-4549-a9f1-8b00aec3d6f0
sda
├─sda1       ext4        1.0       BOOT   1b3a5f5e-e8ed-4cda-8d50-0fa907f4e3a8  733,8M  13% /boot
├─sda2
├─sda5       LVM2_member LVM2 001   V9drnF-wXYq-R12U-WJwp-vzci-f9Br-elnank
│   └─VG_PROXMOX-VG_ROOT ext4        1.0       ROOT   a0d2537d-4bc6-48a3-9977-2c9226448538  3,5G   60% /
│       └─VG_PROXMOX-VG_DATA ext4        1.0       DATA  81099dd7-2743-4279-9834-5357be6d1142  9,3G   44% /var/lib/vz
│           └─VG_PROXMOX-VG_SWAP swap        1         46fbc147-62e0-4513-9dde-858c7fc59463
└─sr0
root@debian:~#
```

La sortie de votre commande `ls -l /var/lib/vz/images/` indique qu'il y a des répertoires pour les conteneurs ou VMs, numérotés 100, 101, 102, 103 et 104. Chacun de ces répertoires correspond à un conteneur que j'ai créé et à la machine pfsense sur proxmox.

`ls -l /var/lib/vz/images/100/`

Cette commande affiche les fichiers à l'intérieur du répertoire pour le conteneur ou la VM avec l'ID 100. Cela signifie que le conteneur utilise bien l'espace de stockage sur le volume LVM VG\_DATA configuré dans VG\_PROXMOX, car /var/lib/vz est l'endroit par défaut où Proxmox stocke ces images lorsqu'il est configuré avec le stockage LVM

```

Sys. de fichiers      Taille Utilisé Dispo Uti% Monté sur
udev                  3,3G      0   3,3G   0% /dev
tmpfs                  686M      1,8M  684M   1% /run
/dev/mapper/VG_PROXMOX-VG_ROOT 10G      6,1G   3,5G  64% /
tmpfs                  3,4G      46M   3,4G   2% /dev/shm
tmpfs                  5,0M      8,0K   5,0M   1% /run/lock
/dev/sda1              920M     123M   734M  15% /boot
/dev/mapper/VG_PROXMOX-VG_DATA 19G      9,0G   8,3G  53% /var/lib/vz
/dev/fuse              128M      20K   128M   1% /etc/pve
tmpfs                  686M     124K   686M   1% /run/user/1000
tmpfs                  686M      48K   686M   1% /run/user/0

root@debian:~# ls -l /var/lib/vz/images/
total 20
drwxr----- 2 root root 4096 21 mars 00:16 100
drwxr----- 2 root root 4096 21 mars 00:26 101
drwxr----- 2 root root 4096 21 mars 12:46 102
drwxr----- 2 root root 4096 21 mars 13:34 103

```

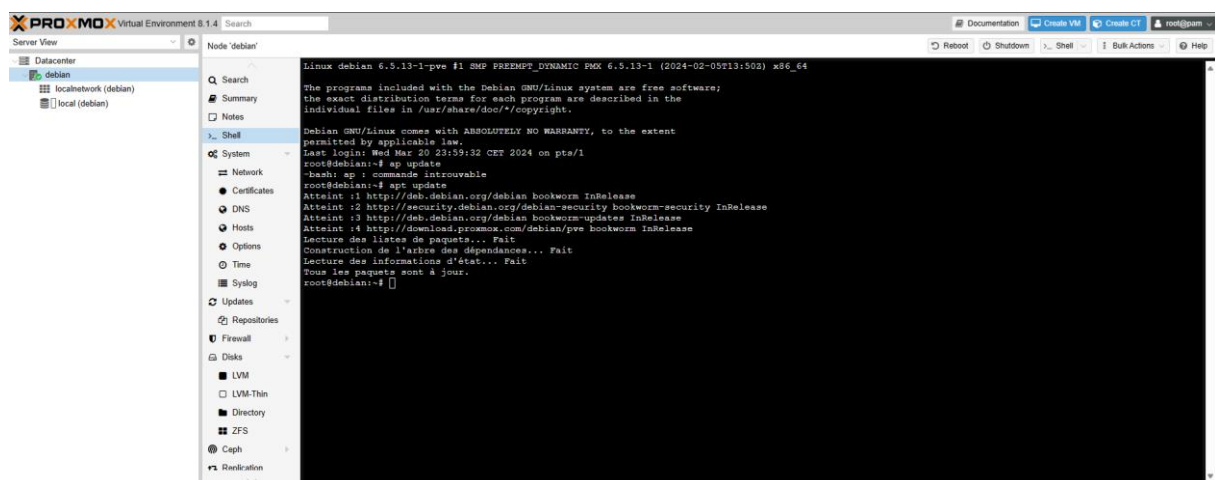
```

root@debian:/var/lib# ls -l /var/lib/vz/images/100/
total 1370240
-rw-r----- 1 root root 9663676416 24 mars 13:10 vm-100-disk-0.raw
root@debian:/var/lib#

```

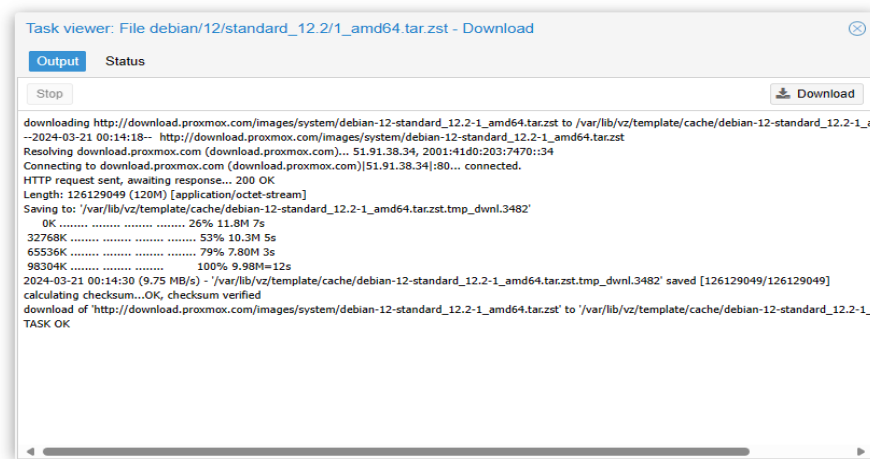
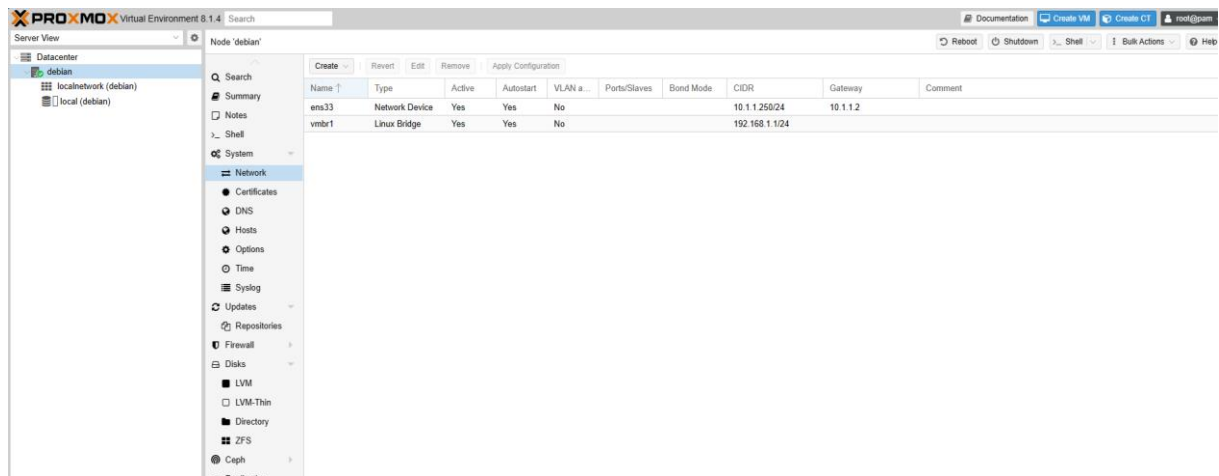
Ensuite j'ai commencé par installer Debian 12 Bookworm, en veillant à configurer une IP fixe et à sélectionner seulement les utilitaires système standard et le serveur SSH. J'ai ensuite assuré que le nom d'hôte était correctement résolu via /etc/hosts. Après l'installation, j'ai ajouté les dépôts et clés de Proxmox VE, mis à jour et upgradé le système, puis installé le noyau Proxmox VE et redémarré. J'ai finalement installé les paquets nécessaires pour Proxmox VE, supprimé le noyau par défaut de Debian et accédé à l'interface web de Proxmox VE pour finaliser la configuration également j'ai dû mettre les droit à mon user en faisant la commande « su » et ensuite « sudo visudo » et ensuite mettre les droits.

Après l'installation de proxmox j'ai accédé à l'interface graphique de celle celle-ci :

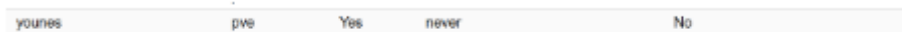


Ensuite j'ai mis à jour mon proxmox , et également mis une adresse IP statique , j'ai créé également un Bridge et télécharger un template de debian12 pour mes

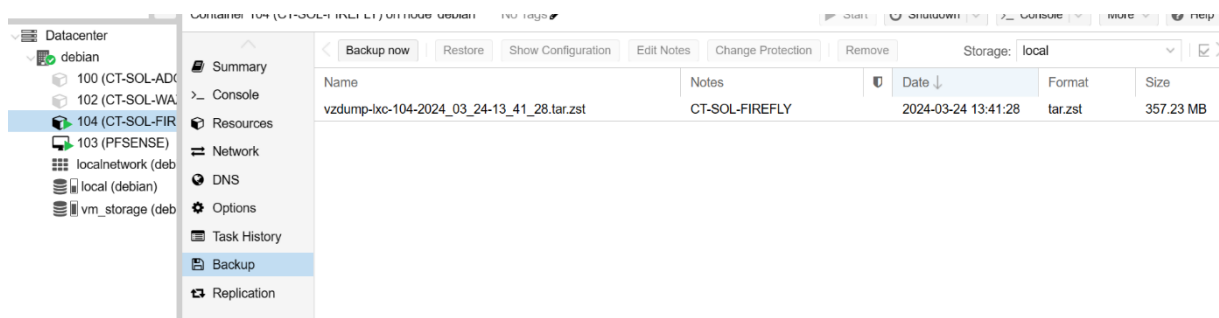
conteneurs. L'objectif est d'avoir un réseau local avec 10.1.1.0/24 et un sous réseau qui est 192.168.1.0/24 :



Création également de mon user :



Et aussi la création de snapshot pour les différentes machines voici un exemple :



Ensuite j'ai commencé à créer mon premier conteneur qui est Adguard ( CT-SOL-ADGUARD ) ainsi j'ai suivi les étapes d'installation :

Je regarde sa connectivité avec internet et l'hôte proxmox :

```
Debian GNU/Linux 12 CT-SOL-ADGUARD tty1

CT-SOL-ADGUARD login: root
Password:
Linux CT-SOL-ADGUARD 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50z) 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.
root@CT-SOL-ADGUARD:~# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eth0@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:32:02:2f brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.1.12/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe32:22f/64 scope link
        valid_lft forever preferred_lft forever
root@CT-SOL-ADGUARD:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=5.24 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=6.79 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 5.240/6.017/6.794/0.777 ms
root@CT-SOL-ADGUARD:~# ping 10.1.1.250
PING 10.1.1.250 (10.1.1.250) 56(84) bytes of data.
64 bytes from 10.1.1.250: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 10.1.1.250: icmp_seq=2 ttl=64 time=0.081 ms
^C
```

On continue l'installation :

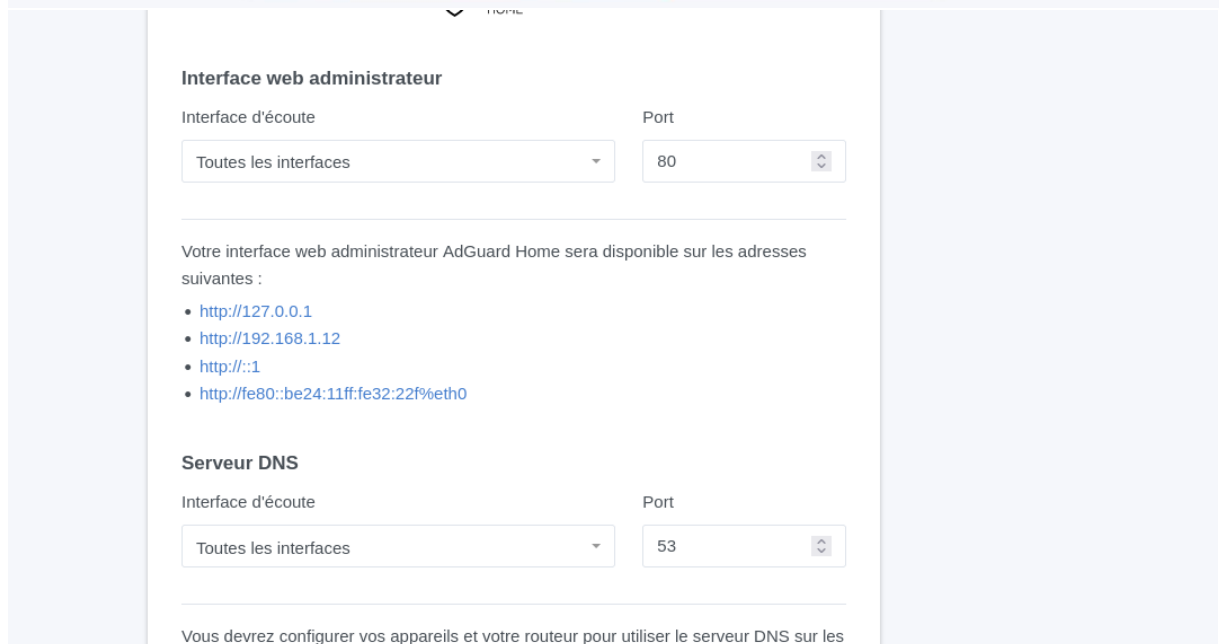
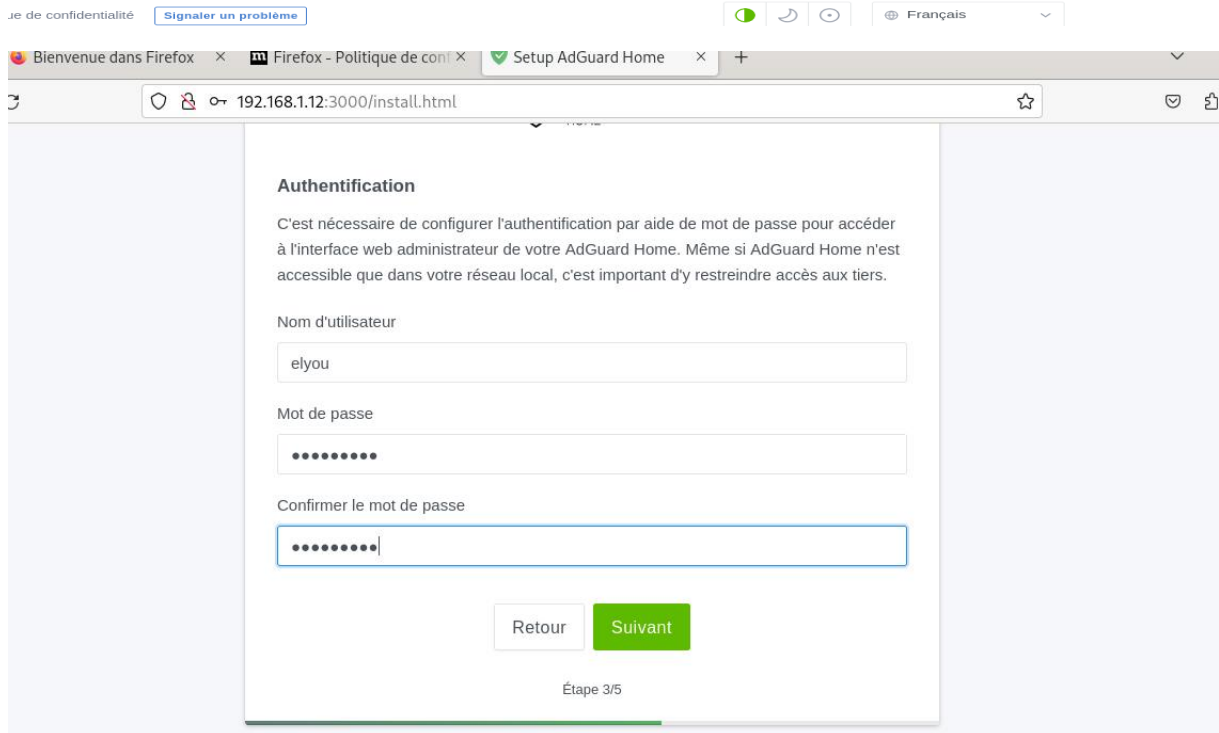
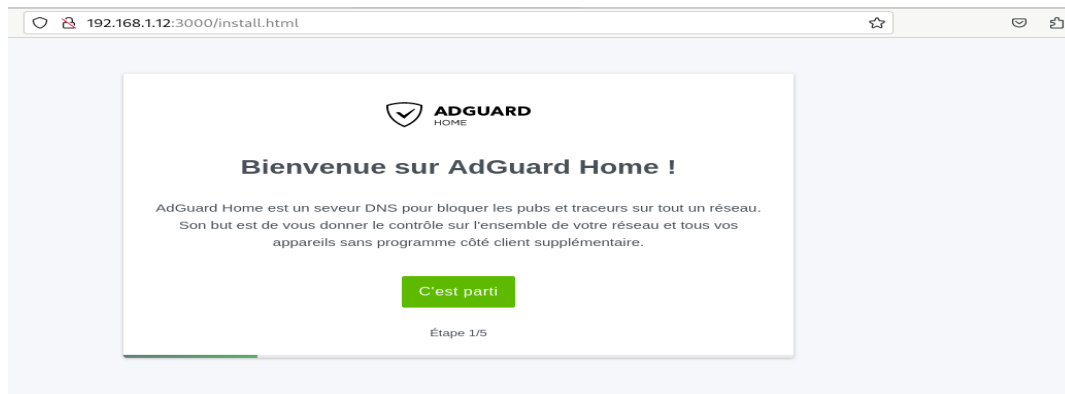
```
2024-03-20 23:18:30 (2.27 MB/s) - 'AdGuardHome_linux_amd64.tar.gz' saved [10643048/10643048]

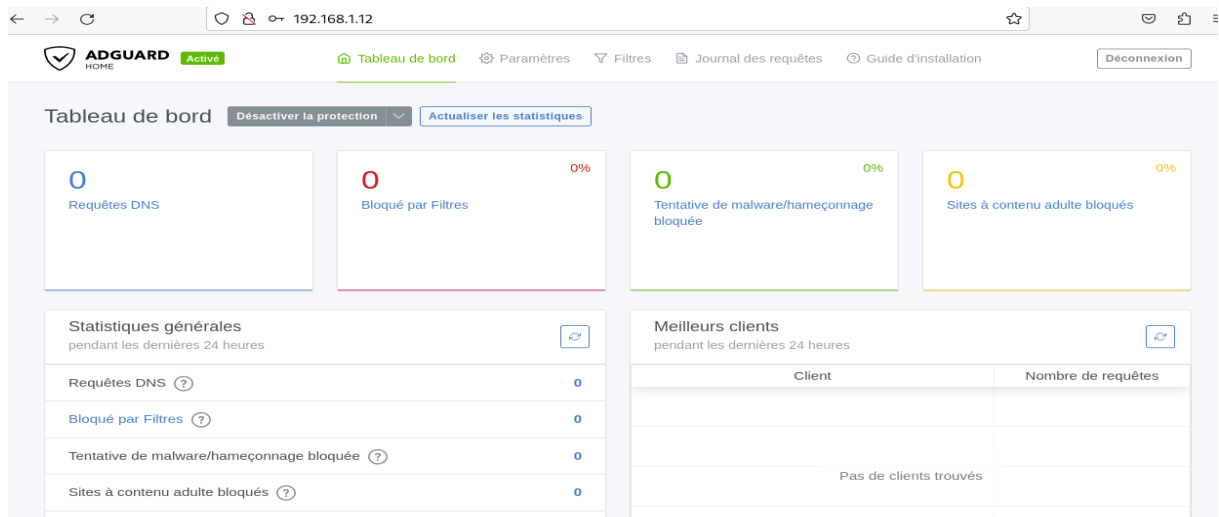
./AdGuardHome/
./AdGuardHome/AdGuardHome
./AdGuardHome/LICENSE.txt
./AdGuardHome/AdGuardHome.sig
./AdGuardHome/README.md
./AdGuardHome/CHANGELOG.md
root@CT-SOL-ADGUARD:~# ls
AdGuardHome  AdGuardHome_linux_amd64.tar.gz
root@CT-SOL-ADGUARD:~#
```

```
AdGuard Home is now available at the following addresses:
2024/03/20 23:19:03 [info] go to http://127.0.0.1:3000
2024/03/20 23:19:03 [info] go to http://[::1]:3000
2024/03/20 23:19:03 [info] go to http://192.168.1.12:3000
2024/03/20 23:19:03 [info] go to http://[fe80::be24:11ff:fe32:22f%eth0]:3000
2024/03/20 23:19:03 [info] service: action install has been done successfully on linux-systemd
root@CT-SOL-ADGUARD:~#
```

Ainsi j'ai obtenu cette interface graphique :



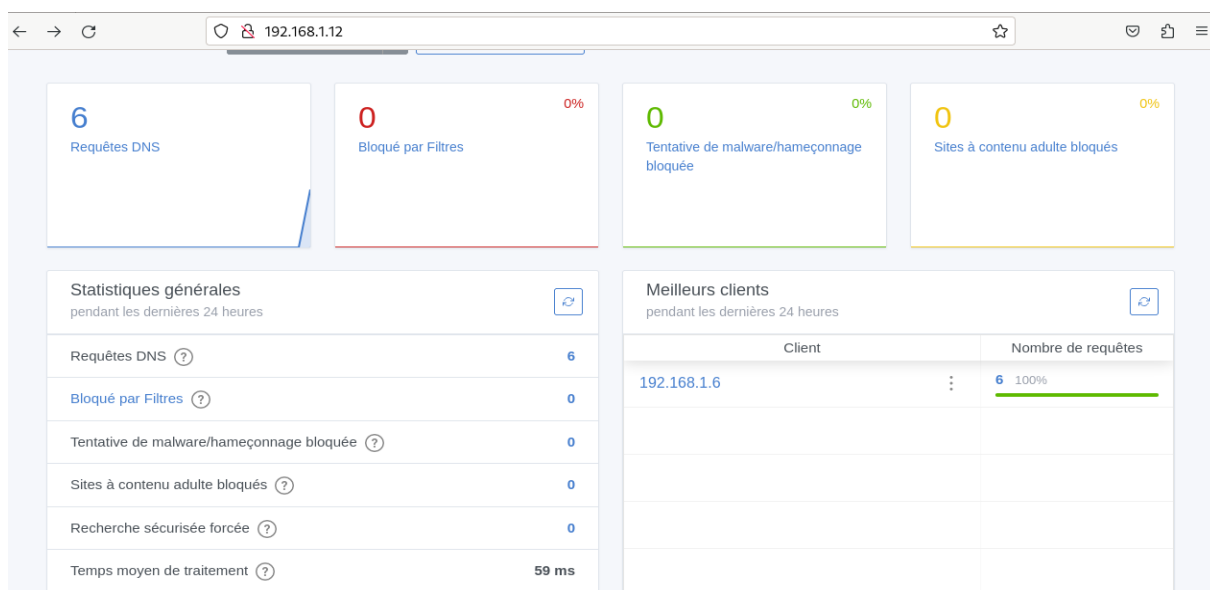




Afin d'avoir un client pour Adguard j'ai dans un premier temps fait le test sur une machine test AdGUARD-Client (ADGUARD-CLIENT) afin d'éviter un problème, j'ai donc modifié le fichier /etc/resolv.conf et mis pour le nameserver L'IP de mon conteneur Adguard 192.168.1.12 voici le résultat :

```
GNU nano 7.2 /etc/resolv.conf *
# --- BEGIN PVE ---
search localdomain
nameserver 192.168.1.12
# --- END PVE ---
```

Temps	Requête	Réponse	Client
00:29:23 21/03/2024	debian.map.fastlydns.net Type: AAAA, DNS brut	Traité 52 ms	192.168.1.6
00:29:23 21/03/2024	debian.map.fastlydns.net Type: A, DNS brut	Traité 50 ms	192.168.1.6
00:29:23 21/03/2024	debian.map.fastlydns.net Type: AAAA, DNS brut	Traité 50 ms	192.168.1.6
00:29:23 21/03/2024	debian.map.fastlydns.net Type: A, DNS brut	Traité 50 ms	192.168.1.6
00:29:23 21/03/2024	_http._tcp.security.debian.org Type: SRV, DNS brut	Traité 75 ms	192.168.1.6
00:29:23 21/03/2024	_http._tcp.deb.debian.org Type: SRV, DNS brut	Traité 72 ms	192.168.1.6



Datcenter

debian

100 (CT-SOL-ADGUARD)

101 (ADGUARD-CLIENT)

localnetwork (debian)

local (debian)

Summary

Console

Resources

Network

DNS

Options

Task History

Backup

Replication

Snapshots

Firewall

Permissions

```
root@ADGUARD-CLIENT:~# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eth@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:be:74:49 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.1.6/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febe:7449/64 scope link
        valid_lft forever preferred_lft forever
root@ADGUARD-CLIENT:~#
```

```
root@ADGUARD-CLIENT:~# dig google.com @192.168.1.12

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> google.com @192.168.1.12
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16520
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

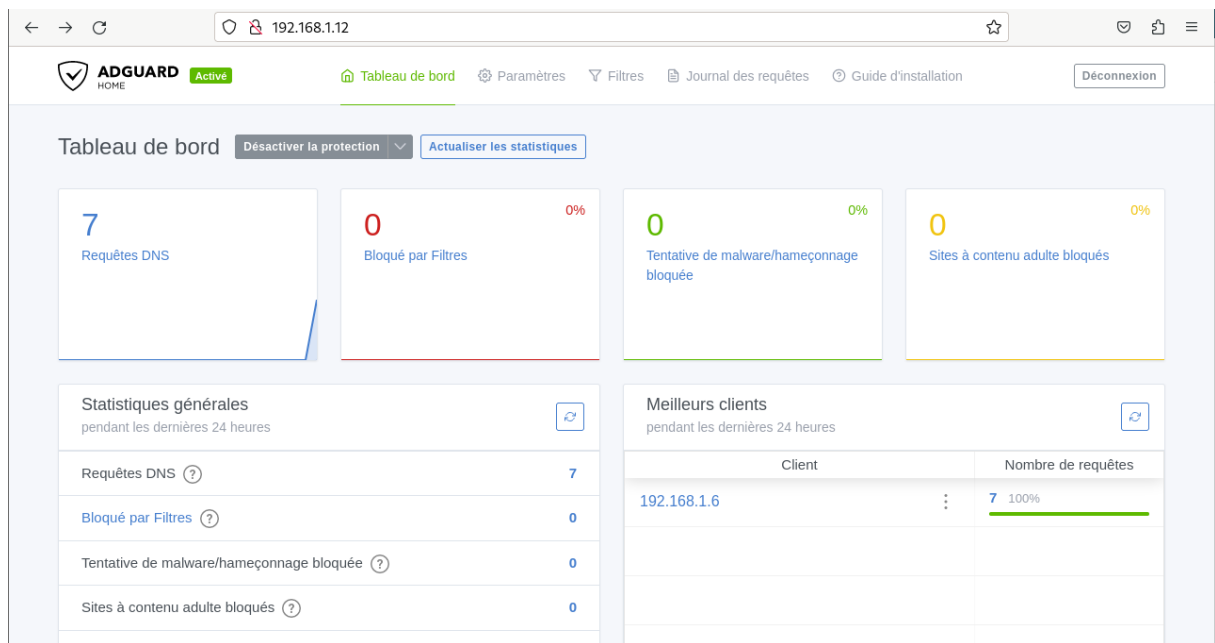
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 66      IN      A      142.250.179.78

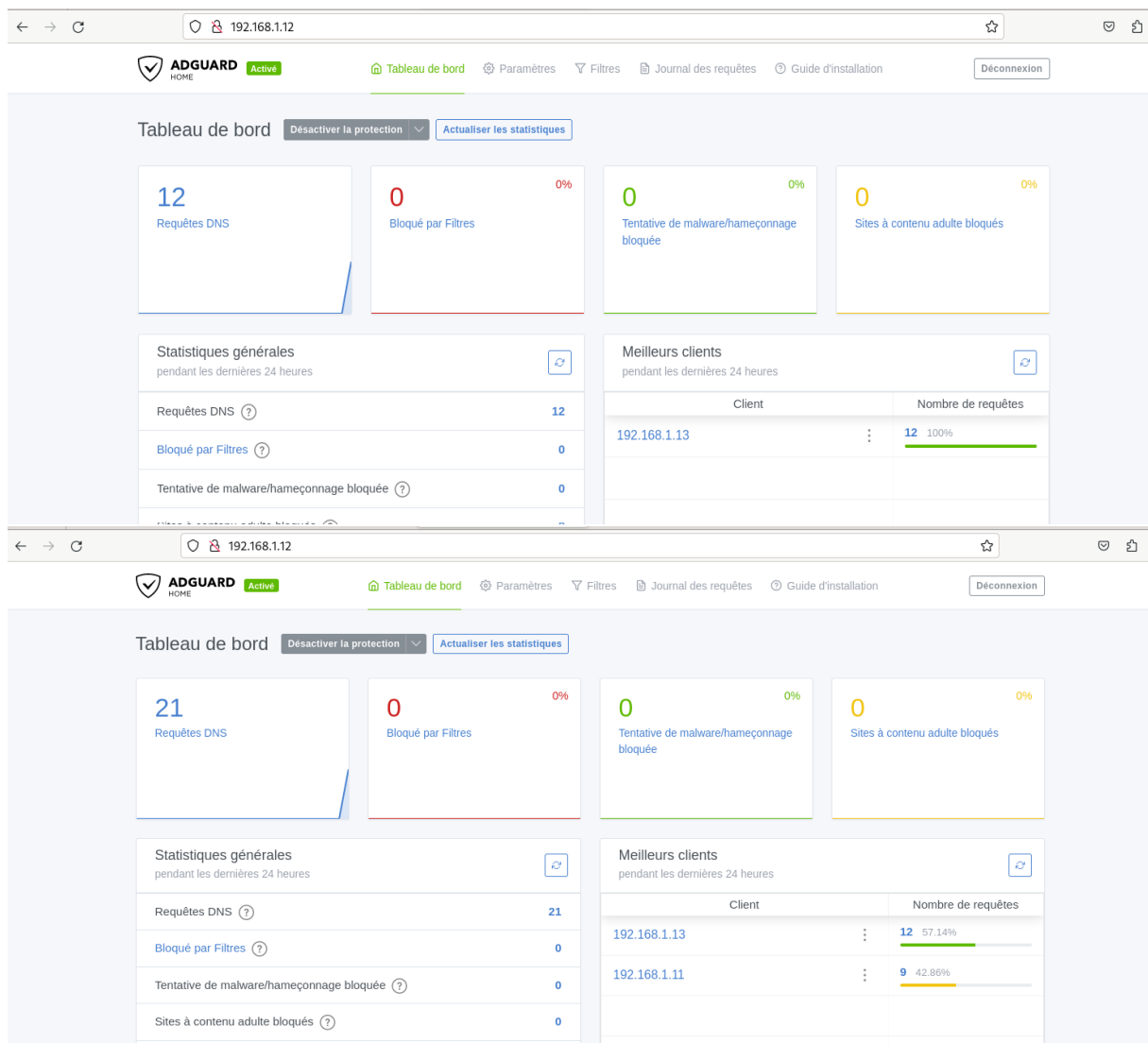
;; Query time: 40 msec
;; SERVER: 192.168.1.12#53(192.168.1.12) (UDP)
;; WHEN: Wed Mar 20 23:34:37 UTC 2024
;; MSG SIZE rcvd: 55

root@ADGUARD-CLIENT:~#
```





Ensuite j'ai fait également la résolution des noms de domaines pour les machines CT-SOL-WAZUH et CT-SOL-FIREFLY avec leurs adresses IP :



Par la suite j'ai créé le deuxième conteneur qui est CT-SOL-WAZUH j'ai suivi également l'installation, dans un premier temps on regarde la connectivité avec l'hôte et internet :

```

CT-SOL-WAZUH login: root
Password:
Linux CT-SOL-WAZUH 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) 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.
root@CT-SOL-WAZUH:~# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eth0@if4: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:1a:4f:c6 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.1.11/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fe1a:4fc6/64 scope link
        valid_lft forever preferred_lft forever
root@CT-SOL-WAZUH:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=6.13 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=6.24 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 101ms
rtt min/avg/max/mdev = 6.131/6.107/6.244/0.056 ms
root@CT-SOL-WAZUH:~# ping 10.1.1.250
PING 10.1.1.250 (10.1.1.250) 56(84) bytes of data.
64 bytes from 10.1.1.250: icmp_seq=1 ttl=64 time=0.120 ms
^C
--- 10.1.1.250 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.120/0.120/0.120/0.000 ms
root@CT-SOL-WAZUH:~#

```

## L'installation finie de wazuh Manager :

```

Active: inactive (dead)
root@CT-SOL-WAZUH:~# systemctl start wazuh-manager
root@CT-SOL-WAZUH:~# systemctl status wazuh-manager
* wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; disabled; preset: enabled)
   Active: active (running) since Thu 2024-03-21 09:52:41 UTC; 3s ago
     Process: 46731 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 118 (limit: 8105)
   Memory: 338.4M
      CPU: 30.300s
   CGroup: /system.slice/wazuh-manager.service
           |-46787 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           |-46828 /var/ossec/bin/wazuh-authd
           |-46842 /var/ossec/bin/wazuh-db
           |-46866 /var/ossec/bin/wazuh-execd
           |-46870 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           |-46873 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           |-46876 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           |-46891 /var/ossec/bin/wazuh-analysisd
           |-46934 /var/ossec/bin/wazuh-syscheckd
           |-46950 /var/ossec/bin/wazuh-remoted
           |-46983 /var/ossec/bin/wazuh-logcollector
           |-47006 /var/ossec/bin/wazuh-monitord
           |-47055 /var/ossec/bin/wazuh-modulesd
Mar 21 09:52:33 CT-SOL-WAZUH env[46731]: Started wazuh-execd...
Mar 21 09:52:33 CT-SOL-WAZUH env[46887]: 2024/03/21 09:52:33 wazuh-analysisd: ERROR: Could not set resource limit for file descriptors to 458752: Operation not permitted
Mar 21 09:52:34 CT-SOL-WAZUH env[46731]: Started wazuh-analysisd...
Mar 21 09:52:35 CT-SOL-WAZUH env[46731]: Started wazuh-syscheckd...
Mar 21 09:52:36 CT-SOL-WAZUH env[46731]: Started wazuh-remoted...
Mar 21 09:52:37 CT-SOL-WAZUH env[46731]: Started wazuh-logcollector...
Mar 21 09:52:38 CT-SOL-WAZUH env[46731]: Started wazuh-monitord...
Mar 21 09:52:39 CT-SOL-WAZUH env[46731]: Started wazuh-modulesd...
Mar 21 09:52:41 CT-SOL-WAZUH env[46731]: Completed.
Mar 21 09:52:41 CT-SOL-WAZUH systemd[1]: Started wazuh-manager.service - Wazuh manager.

```

Après avoir fait l'installation le but était de pouvoir monitorer nos deux autres conteneurs, pour cela j'ai utilisé des agents que j'ai installé sur mes deux autres conteneurs afin de pouvoir communiquer avec mon conteneur Wazuh voici le résultat :

Dans un premier temps il faut que le wazuh-agent fonctionne :

```
* wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; disabled; preset: enabled)
   Active: active (running) since Thu 2024-03-21 10:05:40 UTC; 8s ago
   Process: 4924 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   Tasks: 28 (limit: 8105)
   Memory: 28.5M
   CPU: 1.970s
   CGroup: /system.slice/wazuh-agent.service
           |-4948 /var/ossec/bin/wazuh-execd
           |-4959 /var/ossec/bin/wazuh-agentd
           |-4972 /var/ossec/bin/wazuh-syscheckd
           |-4985 /var/ossec/bin/wazuh-logcollector
           ~-5002 /var/ossec/bin/wazuh-modulesd

Mar 21 10:05:33 ADGUARD-CLIENT systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Mar 21 10:05:33 ADGUARD-CLIENT env[4924]: Starting Wazuh v4.7.3...
Mar 21 10:05:34 ADGUARD-CLIENT env[4924]: Started wazuh-execd...
Mar 21 10:05:35 ADGUARD-CLIENT env[4924]: Started wazuh-agentd...
Mar 21 10:05:36 ADGUARD-CLIENT env[4924]: Started wazuh-syscheckd...
Mar 21 10:05:37 ADGUARD-CLIENT env[4924]: Started wazuh-logcollector...
Mar 21 10:05:38 ADGUARD-CLIENT env[4924]: Started wazuh-modulesd...
Mar 21 10:05:40 ADGUARD-CLIENT env[4924]: Completed.
Mar 21 10:05:40 ADGUARD-CLIENT systemd[1]: Started wazuh-agent.service - Wazuh agent.
```

On modifie le fichier ossec.conf en mettant l'adresse du wazuh manager :

```
root@ADGUARD-CLIENT:~# dig google.com @192.168.1.12

; <<>> DiG 9.18.19-1-deb12ul-Debian <<>> google.com @192.168.1.12
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 16520
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 66      IN      A      142.250.179.78

;; Query time: 40 msec
;; SERVER: 192.168.1.12#53(192.168.1.12) (UDP)
;; WHEN: Wed Mar 20 23:34:37 UTC 2024
;; MSG SIZE rcvd: 55

root@ADGUARD-CLIENT:~#
```

Ensuite il faudra utiliser une clé qui est généré par le wazuh manager afin de pouvoir relier mes conteneurs agent à l'hôte :

```
*****
Wazuh v4.7.3 Agent manager.
The following options are available:
*****

(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: CT-SOL-ADGUARD, IP: any
Provide the ID of the agent to extract the key (or 'q' to quit): 001

Agent key information for '001' is:
DAXIENULVNPTC1BREdVQVJEIGFueSaxZjUzNGMxNTBlNDBkMjQzZWMyYWE1OWU0M2E0NGQwNTEyZWEzZGM4MmFiN2IyM2NhoThlyjQ2ZWMyZGOGNkYjNk

* Press ENTER to return to the main menu.
```

Pour CT-SOL-ADGUARD :

```
root@CT-SOL-ADGUARD:~# /var/ossec/bin/manage_agents -i "MDAxIENULVNPTC1BREdVQVJEIGFueSaxZjUzNGMxNTBlNDBkMjQzZWMyYWE1OWU0M2E0NGQwNTEyZWEzZGM4MmFiN2IyM2NhoThlyjQ2ZWMyZGOGNkYjNk"

Agent information:
  ID:001
  Name:CT-SOL-ADGUARD
  IP Address:any

Confirm adding it?(y/n): Y
Added.
root@CT-SOL-ADGUARD:~#
```

```

*****
* Wazuh v4.7.3 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: L

Available agents:
  ID: 001, Name: CT-SOL-ADGUARD, IP: any

** Press ENTER to return to the main menu.

```

Pour CT-SOL-FIREFLY :

```

root@CT-SOL-FIREFLY:/var/ossec/etc# /var/ossec/bin/manage_agents -i "MDAyIENULVNPTClGSUVFRkx2IDE5Mi4xNjguMS4xMyAyNDI2M2U4OTJlYzNjZWQOMzJlOWI3NWl4NzkxTUKNTFiNzk3YTAlMmM5Y2QxZjZlOThiMjMjPi"

Agent information:
  ID:002
  Name:CT-SOL-FIREFLY
  IP Address:192.168.1.13

Confirm adding it?(y/n): y
Added.
root@CT-SOL-FIREFLY:/var/ossec/etc#

```

On remarque que les deux autres conteneurs son monitorer par le conteneur wazuh ainsi les logs peuvent remontés :

```

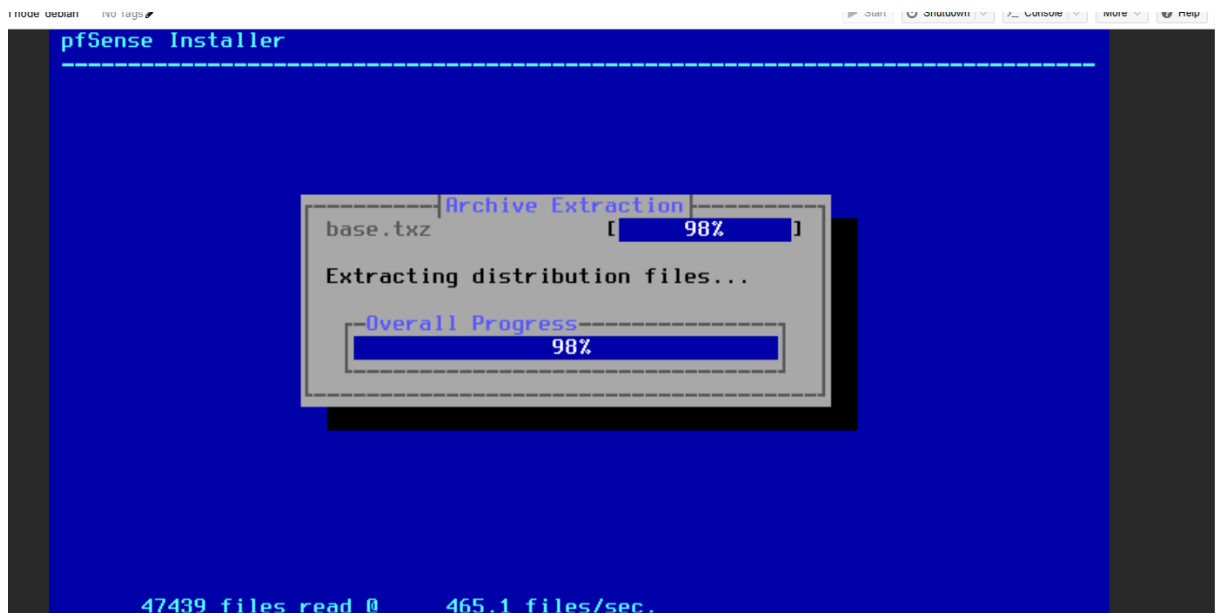
root@CT-SOL-WAZUH:~# /var/ossec/bin/agent_control -lc

Wazuh agent_control. List of available agents:
  ID: 000, Name: CT-SOL-WAZUH (server), IP: 127.0.0.1, Active/Local
  ID: 001, Name: CT-SOL-ADGUARD, IP: any, Active
  ID: 002, Name: CT-SOL-FIREFLY, IP: 192.168.1.13, Active

root@CT-SOL-WAZUH:~#

```

Ensuite l'objectif était de mettre en place Pfsense qui est un parefeu et qui va nous permettre de filtrer les entrées et sorties, après avoir mis l'image de pfsense je fais l'installation dans une machine virtuelle avec deux network devices un vmbr0 pour le WAN et e vmbr1 pour la LAN et je suis la procédure :



Arrivé ici on a une adresse pour le vmbr1 par défaut je décide de changer cette adresse en 192.168.1.7 et ensuite je me connecte à l'interface graphique de pfsense et je suis les étapes :

```
pfSense - Netgate Device ID: 73c98f4f77a3a22f0d11
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.1.1.135/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.7/24

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
```



```
6) Halt system
7) Ping host
8) Shell
15) Restore recent configuration
16) Restart PHP-FPM
```

Enter an option: 7

Enter a host name or IP address: google.fr

```
PING google.fr (172.217.18.195): 56 data bytes
64 bytes from 172.217.18.195: icmp_seq=0 ttl=128 time=11.874 ms
64 bytes from 172.217.18.195: icmp_seq=1 ttl=128 time=9.067 ms
64 bytes from 172.217.18.195: icmp_seq=2 ttl=128 time=11.044 ms
```

```
--- google.fr ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.067/10.662/11.874/1.177 ms
```

Press ENTER to continue.

← → ↻ [https://192.168.1.7/wizard.php?xml=setup\\_wizard.xml](https://192.168.1.7/wizard.php?xml=setup_wizard.xml) 📄 ☆ 📄 📄 📄

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / General Information ?

Step 2 of 9

### General Information

On this screen the general pfSense parameters will be set.

**Hostname**   
Name of the firewall host, without domain part.  
Examples: pfsense, firewall, edgefw

**Domain**   
Domain name for the firewall.  
Examples: home.arpa, example.com

Do not end the domain name with 'local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD.  
[Alternative workarounds for these cases if local TLD is not desired are available.](#)

COMMUNITY EDITION

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

### Time Server Information

Please enter the time, date and time zone.

**Time server hostname**   
Enter the hostname (FQDN) of the time server.

**Timezone**

» Next

## Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType DHCP

## General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

## Static IP Configuration

IP Address

Subnet Mask 32

Upstream Gateway

connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

## RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

## Block bogon networks

Block bogon networks

☐ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

## Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address 192.168.1.7

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask 24

>> Next







Wizard completed.

Check for updates

[Click here](#) to learn about Netgate 24/7/365 support services.

### Anonymous User Survey

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)

Interfaces			
 WAN		10Gbase-T <full-duplex>	10.1.1.135
 LAN		10Gbase-T <full-duplex>	192.168.1.7

WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

On se dirige vers les règles afin de voir si elles sont valides pour l'intitulé de l'exercice :

ANY:ANY par défaut : Cela implique que j'ai laissé les règles de pare-feu en place pour autoriser tout le trafic depuis et vers le LAN sans restrictions spécifiques. C'est la configuration typique pour un pare-feu par défaut, permettant à tous les types de trafic de traverser le pare-feu

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/995 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Le mode automatique est sélectionné, ce qui permet de générer automatiquement les règles NAT pour le trafic sortant du réseau local. Deux règles automatiques sont affichées : l'une pour le trafic ISAKMP et l'autre pour le trafic général sortant. Ces règles sont configurées pour que le trafic provenant de mon réseau local (192.168.1.0/24) soit traduit pour sortir avec l'adresse IP publique du WAN lorsqu'il accède à Internet.

Port Forward 1:1 Outbound NAT

Outbound NAT Mode

Mode

Automatic outbound NAT rule generation. (IPsec passthrough included)

Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
Add  Add  Delete  Toggle  Save										

Automatic Rules

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 192.168.1.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 192.168.1.0/24	*	*	*	WAN address	*		Auto created rule

Interfaces

WAN		10Gbase-T <full-duplex>	10.1.1.135
LAN		10Gbase-T <full-duplex>	192.168.1.7

On confirme que le NAT fonctionne correctement car l'adresse IP publique visible sur Internet (37.65.161.23) est différente de l'adresse IP privée du pare-feu (10.1.1.135). Cela montre que pfSense agit comme une passerelle efficace et que le trafic sortant est correctement en place pour accéder à Internet.

Le pfSense avec l'adresse WAN 10.1.1.135 agit comme le point d'entrée pour le réseau LAN (192.168.1.0). Cela signifie que tout le trafic entrant et sortant doit passer par pfSense, qui gère le NAT, les règles de pare-feu, et d'autres aspects de la sécurité et de la connectivité réseau.

```
root@CT-SOL-ADGUARD:~# traceroute google.com
traceroute to google.com (142.250.201.174), 30 hops max, 60 byte packets
 1  192.168.1.7 (192.168.1.7)  3.323 ms  3.636 ms  3.821 ms
 2  10.1.1.2 (10.1.1.2)  15.090 ms  21.433 ms  21.564 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
```

```
root@CT-SOL-ADGUARD:~# curl ifconfig.me
37.65.161.23root@CT-SOL-ADGUARD:~#
```

Après avoir installé pfsense , j'avais changé la passerelle pour le LAN donc pour mes conteneurs il faudra qu'ils changent de passerelle afin de pouvoir communiquer avec internet :

Et enfin j'ai installé mon conteneur Firefly ( CT-SOL-FIREFLY ) j'ai également suivi l'installation avec les différentes commandes :

Dans un premier temps on vérifie la connectivité :

```

CT-SOL-FIREFLY login: root
Password:
Linux CT-SOL-FIREFLY 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) 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.
root@CT-SOL-FIREFLY:~# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eth0@if33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:2c:5b:d2 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.1.13/25 brd 192.168.1.127 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe2c:5bd2/64 scope link
        valid_lft forever preferred_lft forever
root@CT-SOL-FIREFLY:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=29.6 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 29.621/29.621/29.621/0.000 ms
root@CT-SOL-FIREFLY:~# ping 10.1.1.250
PING 10.1.1.250 (10.1.1.250) 56(84) bytes of data.
64 bytes from 10.1.1.250: icmp_seq=1 ttl=63 time=3.86 ms
^C
--- 10.1.1.250 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.857/3.857/3.857/0.000 ms

```

## Ensuite l'installation :

```

Reading state information... Done
The following NEW packages will be installed:
  php8.0-mysql
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 121 kB of archives.
After this operation, 466 kB of additional disk space will be used.
Get:1 https://packages.sury.org/php bookworm/main amd64 php8.0-mysql amd64 1:8.0.30-2+0~20230904.59+debian12~1.gbp806e95 [121 kB]
Fetched 121 kB in 0s (718 kB/s)
Selecting previously unselected package php8.0-mysql.
(Reading database ... 23194 files and directories currently installed.)
Preparing to unpack .../php8.0-mysql_1:8.0.30-2+0~20230904.59+debian12~1.gbp806e95_amd64.deb ...
Unpacking php8.0-mysql (1:8.0.30-2+0~20230904.59+debian12~1.gbp806e95) ...
Setting up php8.0-mysql (1:8.0.30-2+0~20230904.59+debian12~1.gbp806e95) ...

Creating config file /etc/php/8.0/mods-available/mysqlnd.ini with new version

Creating config file /etc/php/8.0/mods-available/mysqli.ini with new version

Creating config file /etc/php/8.0/mods-available/pdo_mysql.ini with new version
Processing triggers for libapache2-mod-php8.0 (1:8.0.30-2+0~20230904.59+debian12~1.gbp806e95) ...
Processing triggers for php8.0-cli (1:8.0.30-2+0~20230904.59+debian12~1.gbp806e95) ...
root@CT-SOL-FIREFLY:~# php -v
PHP 8.0.30 (cli) (built: Sep  4 2023 08:12:32) ( NTS )
Copyright (c) The PHP Group
Zend Engine v4.0.30, Copyright (c) Zend Technologies
    with Zend OPcache v8.0.30, Copyright (c), by Zend Technologies
root@CT-SOL-FIREFLY:~#

```

```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE firefly_db;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'fireflyuser'@'localhost' IDENTIFIED BY 'azerty';
Query OK, 0 rows affected (0.003 sec)

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

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye
root@CT-SOL-FIREFLY:~# curl -sS https://getcomposer.org/installer -o composer-setup.php
root@CT-SOL-FIREFLY:~# php composer-setup.php --install-dir=/usr/local/bin --filename=composer
All settings correct for using Composer
Downloading...

Composer (version 2.7.2) successfully installed to: /usr/local/bin/composer
Use it: php /usr/local/bin/composer
root@CT-SOL-FIREFLY:~#

```



```

- Installing symfony/polyfill-util (v1.2.0): Extracting archive
- Installing symfony/polyfill-php56 (v1.2.0): Extracting archive
- Installing jeremeamia/SuperClosure (2.2.0): Extracting archive
- Installing doctrine/inferno (v1.1.0): Extracting archive
- Installing classpreloader/classpreloader (3.0.0): Extracting archive
- Installing laravel/framework (v5.3.10): Extracting archive
- Installing barryvdh/laravel-debugbar (v2.3.0): Extracting archive
- Installing symfony/class-loader (v3.1.4): Extracting archive
- Installing barryvdh/reflection-docblock (v2.0.4): Extracting archive
- Installing barryvdh/laravel-ide-helper (v2.2.1): Extracting archive
- Installing davejamesmiller/laravel-breadcrumbs (3.0.1): Extracting archive
- Installing doctrine/lexer (v1.0.1): Extracting archive
- Installing doctrine/annotations (v1.2.7): Extracting archive
- Installing doctrine/cache (v1.6.0): Extracting archive
- Installing doctrine/collections (v1.3.0): Extracting archive
- Installing doctrine/common (v2.6.1): Extracting archive
- Installing doctrine/dbal (v2.5.5): Extracting archive
- Installing laravelcollective/html (v5.3.0): Extracting archive
- Installing league/commonmark (0.15.0): Extracting archive
- Installing league/csv (8.1.1): Extracting archive
- Installing christian-riesen/base32 (1.3.1): Extracting archive
- Installing pragmarx/google2fa (v1.0.1): Extracting archive
- Installing twig/twig (v1.25.0): Extracting archive
- Installing rcrowe/twigbridge (v0.9.3): Extracting archive
- Installing rmccue/requests (v1.6.1): Extracting archive
- Installing watson/validating (3.0.0): Extracting archive
Generating autoload files
Illuminate\Foundation\ComposerScripts::postInstall
php artisan optimize
Generating optimized class loader
Compiling common classes

```

On modifie le fichier de configuration en rentrant les informations que j'ai mis dans la base mysql :

```

GNU nano 7.2 /var/www/firefly-iii/.env *
APP_ENV=production
APP_DEBUG=false
APP_FORCE_SSL=false
APP_FORCE_ROOT=
APP_KEY=SomeRandomStringOf32CharsExactly
APP_LOG_LEVEL=warning
APP_URL=http://localhost

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=firefly
DB_USERNAME=fireflyuser
DB_PASSWORD=azerty

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
QUEUE_DRIVER=sync

COOKIE_PATH="/"
COOKIE_DOMAIN=
COOKIE_SECURE=false

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=mailtrap.io
MAIL_PORT=2525
MAIL_FROM=changeme@example.com
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ENCRYPTION=null

```

```
Do you really wish to run this command? (yes/no) [no]:
> yes
```

```
*****
*      Application In Production!      *
*****
```

```
Do you really wish to run this command? (yes/no) [no]:
> yes
```

Migration table not found.

```
*****
*      Application In Production!      *
*****
```

```
Do you really wish to run this command? (yes/no) [no]:
> yes
```

Migration table created successfully.

```
Migrated: 2016_06_16_000000_create_support_tables
Migrated: 2016_06_16_000001_create_users_table
Migrated: 2016_06_16_000002_create_main_tables
Migrated: 2016_08_25_091522_changes_for_3101
Migrated: 2016_09_12_121359_fix_nullable
```

```
*****
*      Application In Production!      *
*****
```

```
Do you really wish to run this command? (yes/no) [no]:
> yes
```

```
Seeded: AccountTypeSeeder
Seeded: TransactionCurrencySeeder
Seeded: TransactionTypeSeeder
Seeded: PermissionSeeder
Seeded: TestDataSeeder
```

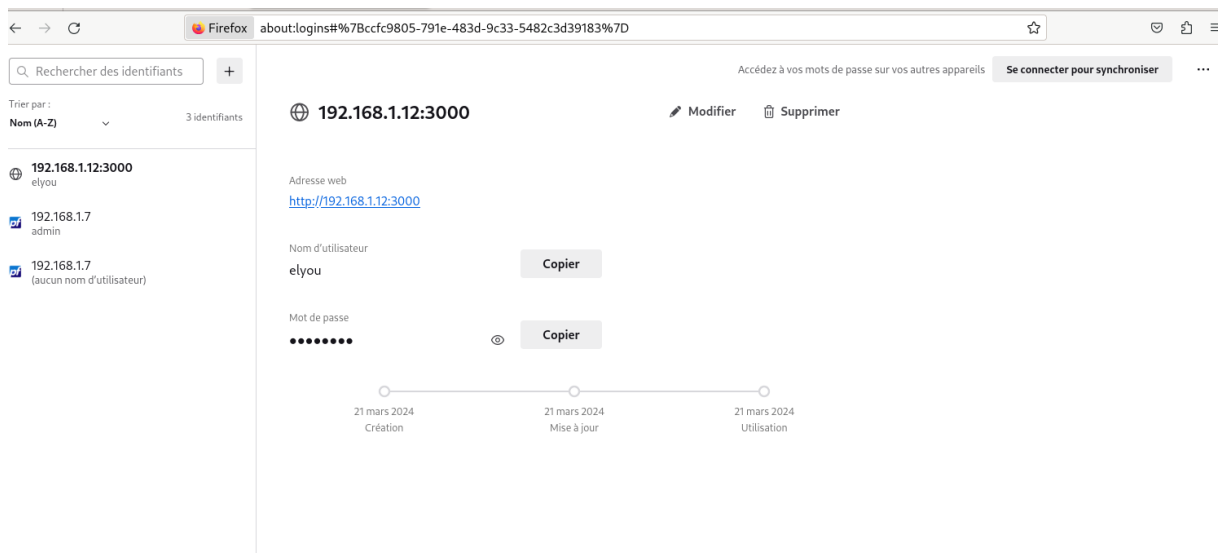
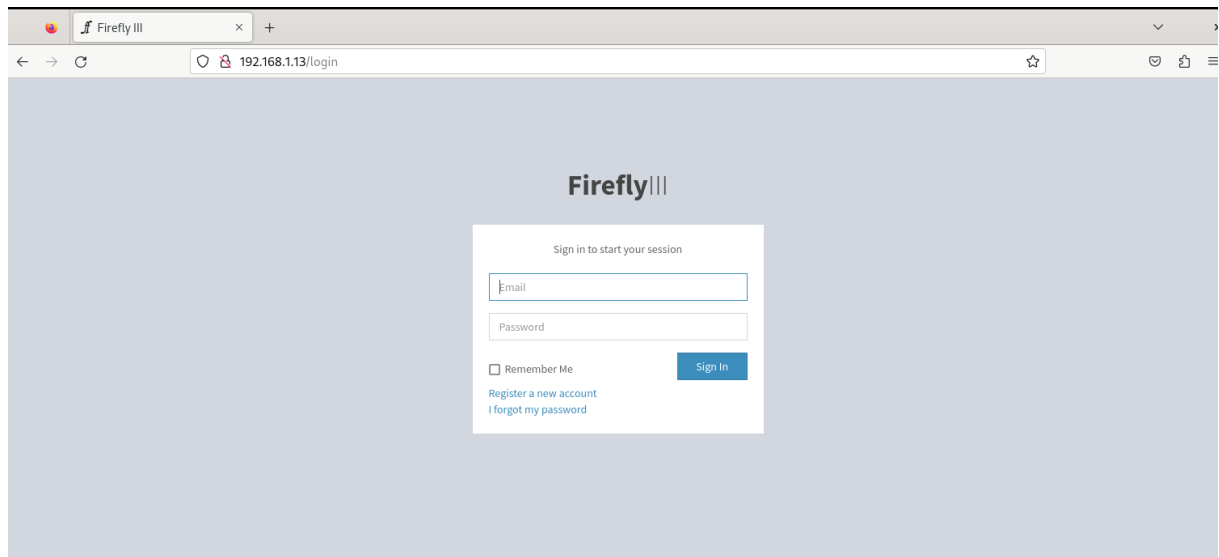
```
root@CT-SOL-FIREFLY:/var/www/firefly-iii# php artisan key:generate
Application key [base64:46bIaHVlOYQNRJrao/Vcq0oltAoW+FmFD38fTG8TvtQ=] set successfully.
root@CT-SOL-FIREFLY:/var/www/firefly-iii#
```

```
root@CT-SOL-FIREFLY:/var/www/firefly-iii# php artisan passport:install
Encryption keys generated successfully.
Personal access client created successfully.
Client ID: 1
Client Secret: 3lRswZWf9uVCs9bVAqaDECsqR66EQbGJTVDsWGP2
Password grant client created successfully.
Client ID: 2
Client Secret: AQQ2TVToEwe3m2JmKbSxhRs1Q3WN5wm4kXKQ7ocy
```

```
root@CT-SOL-FIREFLY:/var/www/firefly-iii# systemctl status nginx
* nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-03-21 16:26:16 UTC; 5s ago
     Docs: man:nginx(8)
    Process: 28031 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 28032 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 28033 (nginx)
      Tasks: 3 (limit: 8105)
     Memory: 2.7M
        CPU: 30ms
    CGroup: /system.slice/nginx.service
            |-28033 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
            |-28034 "nginx: worker process"
            \-28035 "nginx: worker process"

Mar 21 16:26:16 CT-SOL-FIREFLY systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Mar 21 16:26:16 CT-SOL-FIREFLY systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@CT-SOL-FIREFLY:/var/www/firefly-iii#
```

Voici l'interface :



Et juste en dessous ce sont quelques précisions pour la configuration de l'agent wazuh dont j'ai parlé précédent :

```
Wazuh - Agent - Default configuration for debian 12
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.1.11[redacted]/address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>debian, debian12</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client buffer>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sya>yes</check_sya>
  </rootcheck>
</ossec_config>
```

```

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>

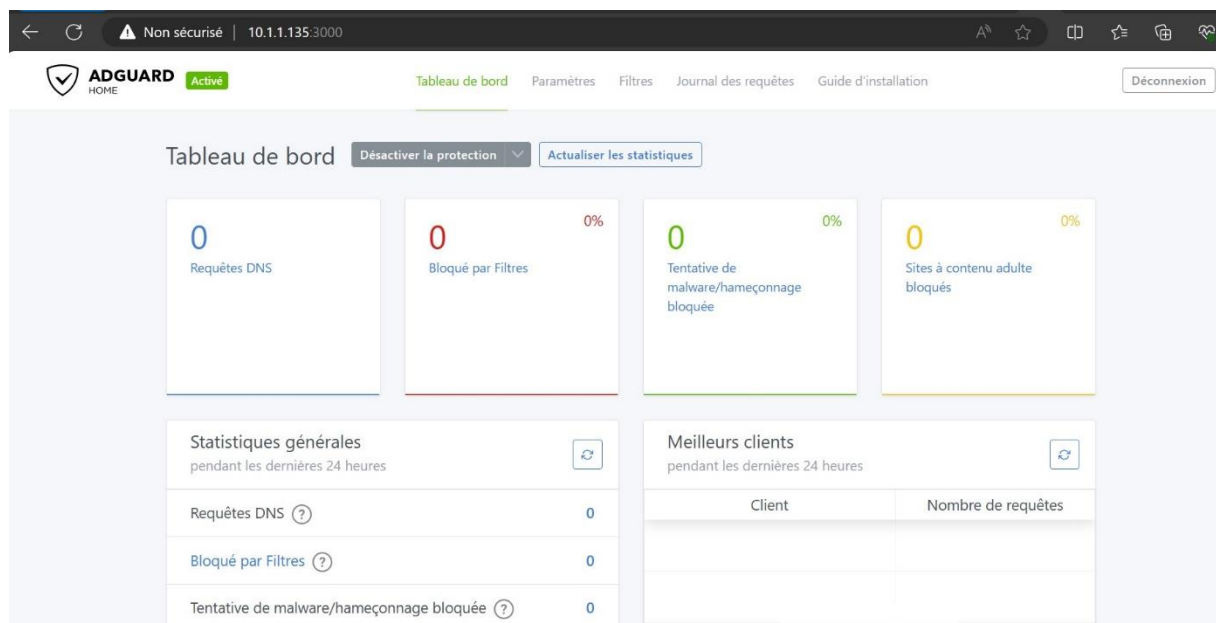
root@CT-SOL-FIREFLY:/var/ossec/etc# systemctl restart wazuh-agent
root@CT-SOL-FIREFLY:/var/ossec/etc# systemctl status wazuh-agent
wazuh-agent.service - Wazuh agent
Loaded: loaded (/lib/systemd/system/wazuh-agent.service; disabled; preset: enabled)
Active: active (running) since Thu 2024-03-21 16:34:33 UTC; 10s ago
Process: 30144 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 29 (limit: 8105)
Memory: 14.7M
CPU: 4.568s
CGroup: /system.slice/wazuh-agent.service
└─30167 /var/ossec/bin/wazuh-execd
└─30178 /var/ossec/bin/wazuh-agentd
└─30190 /var/ossec/bin/wazuh-syscheckd
└─30203 /var/ossec/bin/wazuh-logcollector
└─30221 /var/ossec/bin/wazuh-modulesd

Mar 21 16:34:25 CT-SOL-FIREFLY systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Mar 21 16:34:25 CT-SOL-FIREFLY env[30144]: Starting Wazuh v4.7.3...
Mar 21 16:34:26 CT-SOL-FIREFLY env[30144]: Started wazuh-execd...
Mar 21 16:34:27 CT-SOL-FIREFLY env[30144]: Started wazuh-agentd...
Mar 21 16:34:28 CT-SOL-FIREFLY env[30144]: Started wazuh-syscheckd...
Mar 21 16:34:30 CT-SOL-FIREFLY env[30144]: Started wazuh-logcollector...
Mar 21 16:34:31 CT-SOL-FIREFLY env[30144]: Started wazuh-modulesd...
Mar 21 16:34:33 CT-SOL-FIREFLY env[30144]: Completed.
Mar 21 16:34:33 CT-SOL-FIREFLY systemd[1]: Started wazuh-agent.service - Wazuh agent.
root@CT-SOL-FIREFLY:/var/ossec/etc#

```

Mise en place de la redirection des ports afin de pouvoir accéder à mes services sur mon système hôte :

Dans un premier temps nous allons commencer avec adguard voici l'interface directement sur mon pc hôte avec l'adresse ip wan de mon pfSense 10.1.1.135 et le port configurer :



Voici également la règle NAT que j'ai mis en place :

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPt

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	3000 (HBCI)	192.168.1.12	3000 (HBCI)		

Add
 Add
 Delete
 Toggle
 Save
 Separator

Legend  
 Pass  
 Linked rule

Floating WAN LAN

Rules (Drag to Change Order)												
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	✓	0/1 KiB	IPv4 ICMP any	*	*	WAN address	*	none				
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.1.12	3000 (HBCI)	*	none	NAT		

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

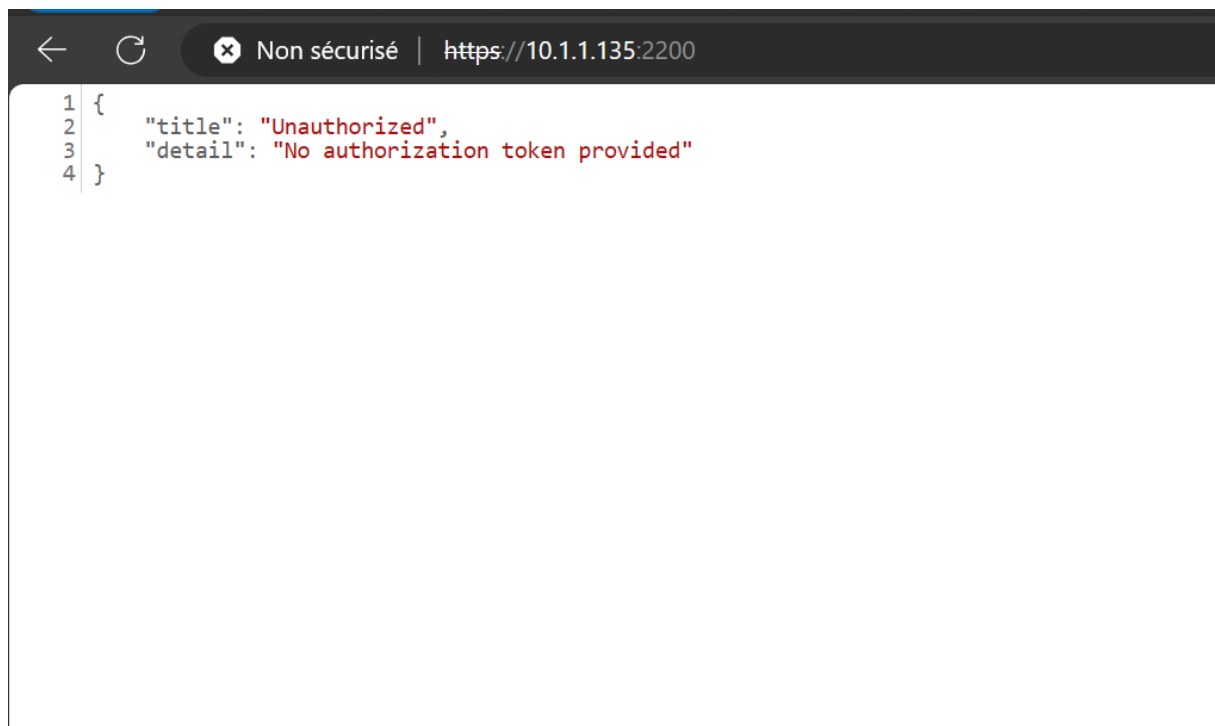
Voici également la communication de mon pc hote avec le wan de psfense :

```
PS C:\Users\user> ping 10.1.1.135

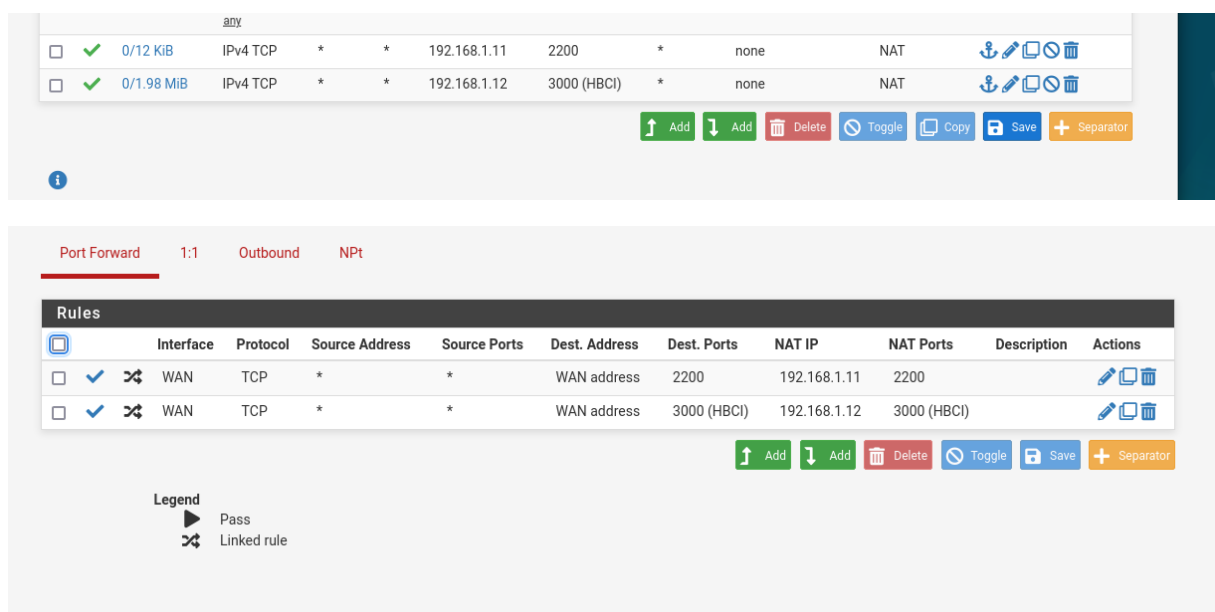
Envoi d'une requête 'Ping' 10.1.1.135 avec 32 octets de données :
Réponse de 10.1.1.135 : octets=32 temps=3 ms TTL=64
Réponse de 10.1.1.135 : octets=32 temps=2 ms TTL=64
Réponse de 10.1.1.135 : octets=32 temps=2 ms TTL=64
Réponse de 10.1.1.135 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 10.1.1.135:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 3ms, Moyenne = 2ms
```

Pour wazuh j'ai obtenu l'interface mais il me manque juste le token à récupérer pour pouvoir afficher l'interface mais on remarque la redirection fonctionne sur le pc hote :

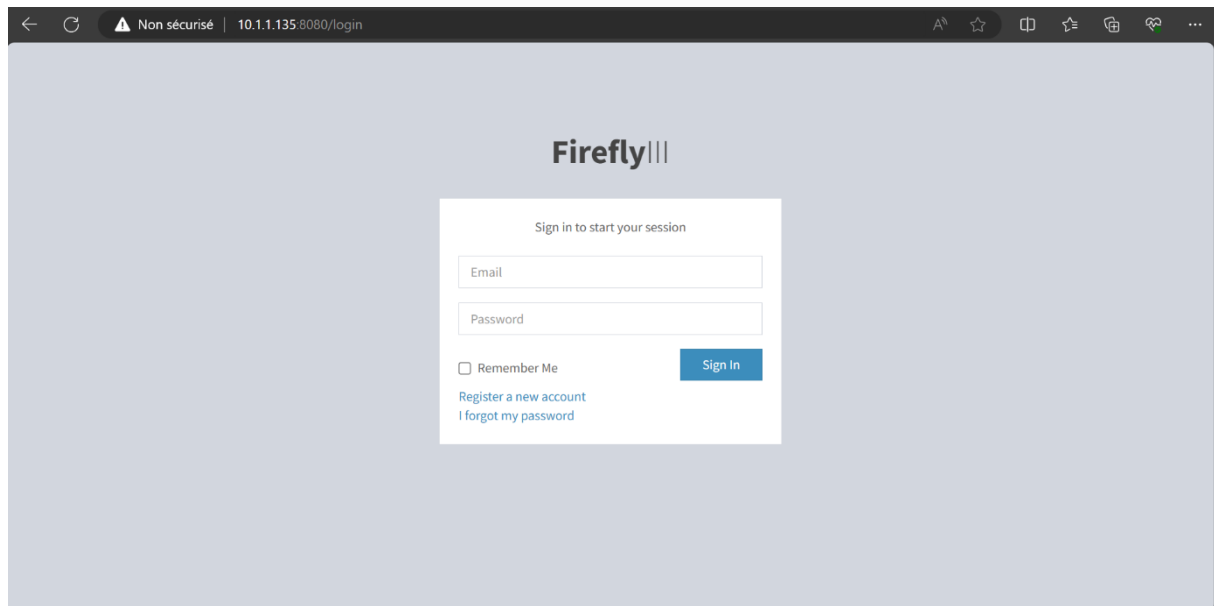


Voici la règle pour la redirection :



Et enfin l'interface de firefly III:





Et voici les règles de redirections :

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	8080	192.168.1.13	8080		

Et également les différentes modifications que j'ai fait pour pouvoir obtenir ce résultat :

```
server {
    listen 8080;
    server_name 192.168.1.13;

    root /var/www/firefly-iii/public;
    index index.php;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
```

```
APP_FORCE_ROOT=
APP_KEY=base64:46bIaHVioYQNRJrao/Vcq0oltAoW+FmFD38fTG8TvtQ=
APP_LOG_LEVEL=warning
APP_URL=http://10.1.1.135:8080
```

```
DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=firefly
DB_USERNAME=fireflyuser
```

Enfin j'ai pu répondre au différent besoin demandé qui correspondait à pouvoir afficher les services sur mon système hôte en faisant des redirections de port via pfsense.

Conclusion :

Montage d'un serveur Proxmox : Le serveur Proxmox a été correctement configuré pour être en contact avec le réseau principal de l'entreprise, offrant une plateforme robuste pour héberger les conteneurs nécessaires.

Configuration de pfSense comme pare-feu et passerelle : Un pare-feu pfSense a été mis en place, laissant la règle ANY:ANY par défaut pour simplifier l'accès initial tout en se concentrant sur l'aspect passerelle de la solution. Cela a créé un point d'entrée sécurisé pour votre sous-réseau.

Déploiement et configuration des conteneurs : Trois conteneurs avec des images Debian standard ont été déployés et configurés pour héberger les solutions suivantes :

- 192.168.1.12 Adguard Home (CT-SOL-ADGUARD) pour le filtrage du contenu DNS,
- 192.168.1.11 Wazuh (CT-SOL-WAZUH) pour la surveillance de la sécurité,
- 192.168.1.13 et optionnellement Firefly III (CT-SOL-FIREFLY) comme solution de gestion financière personnelle.

Connectivité et communication : La vérification a confirmé que le serveur Proxmox peut pinger les conteneurs, indiquant une communication réseau réussie entre eux.

La redirection de ports a été mise en place pour permettre l'accès aux services depuis mon système hôte, en particulier.

L'ensemble du processus a été documenté, et tous les fichiers de configuration nécessaires seront fournis.

