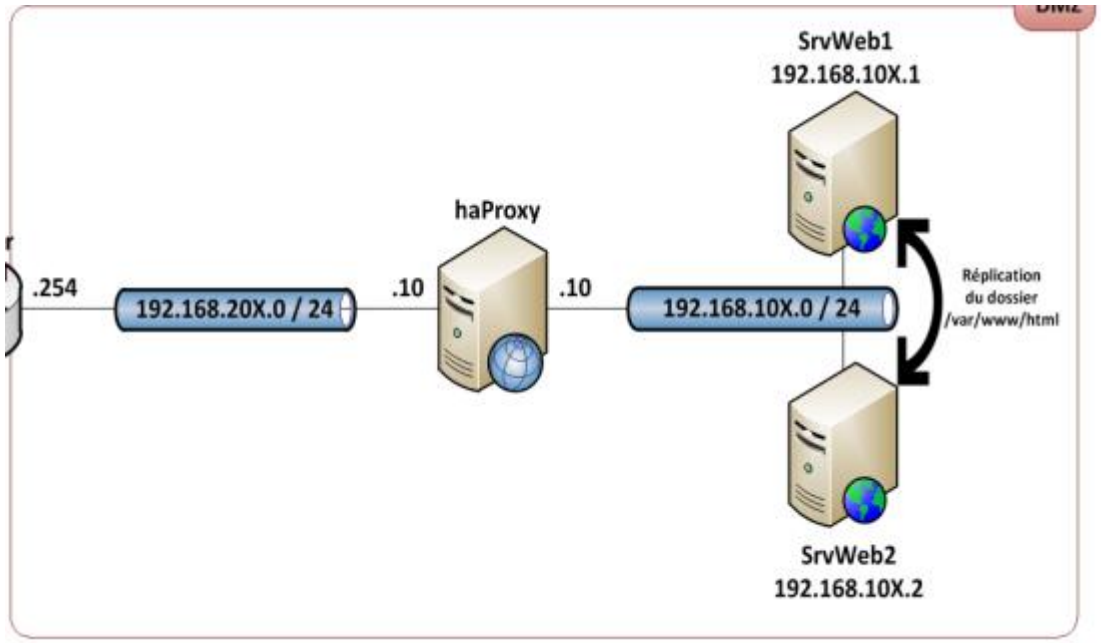
Documentation Haproxy + server web + BDD +PFSENSE

Voici le réseau qui doit être créé :



- Configuration des cartes réseau du serveur haproxy

```
 GNU nano 5.4                                /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 inet static
        address 192.168.219.10/24
        gateway 192.168.219.254

auto ens36
iface ens36 inet static
        address 192.168.119.10/24
```

- Installation de Haproxy

Commande :

  - Apt update
  - Apt install haproxy

- Configuration

Nano /etc/haproxy/haproxy.cfg

```
  GNU nano 5.4                          /etc/haproxy/haproxy.cfg
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd listeners
        stats timeout 30s
        user haproxy
        group haproxy
        daemon

        # Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private

        # See: https://ssl-config.mozilla.org/#server=haproxy&server-version=2.0.3&config=intermedi>
        ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-EC>
        ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_PO>
        ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http



frontend myfrontend
        bind *:80
        mode http
        default_backend mybackend

backend mybackend
        balance roundrobin
        mode http
        cookie SRV_ID insert indirect nocache
        server SrvWeb1 192.168.119.1:80 cookie srv1 check
        server SrvWeb2 192.168.119.2:80 cookie srv1 check
_
```

Redémarrer haproxy

Service haproxy restart

Ces deux parties permettent de mettre en place les cookies

- Création d'un serveur web
  - Commande d'installation

    Apt install apache2

    Apt install php7.4

  - Configuration de la carte réseau

```
  GNU nano 5.4                                /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface


auto ens33
iface ens33 inet static
        address 192.168.119.1/24
        gateway 192.168.119.10
```

  - Commande de création de la page web

    Nano /var/www/html/index.php

    Créer votre page web

- Cloner votre premier serveur web pour créer le deuxième
  - Changer son adresse IP

```
  GNU nano 5.4                          /var/www/html/ConnectBDD.php
<?php
////////////////////////// Connexion à la base de données ////////////////////
try {    $bdd = new PDO('mysql:host=10.20.0.30;dbname=haproxy;', 'root', 'root' array(PDO::MYSQL_A
catch (Exception $e) {     die('Erreur : ' . $e->getMessage()); }
?>
```

Attention mettre à jour les connexions au serveurBDD

- Mise en place du lsyncd sur les deux serveurs web
  - Commande

Apt install lsyncd

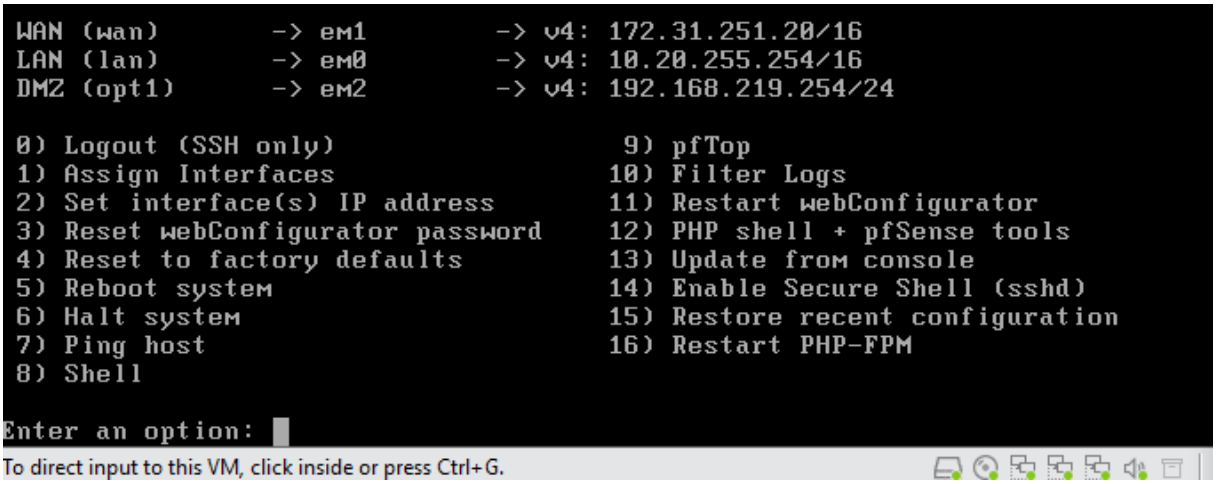
Configuration du lsyncd

Nano /etc/lsyncd/lsyncd.conf.lua

```
  GNU nano 5.4                          /etc/lsyncd/lsyncd.conf.lua
settings {
        logfile = /var/log/lsyncd/lsyncd.log,
        statusFile = /var/log/lsyncd/lsyncd-status.log,
        statusInterval = 1,
        insist = 1
}

sync {
        default.rsyncssh,
        source = /var/www/html,
        host = 192.168.119.2,
        targetdir = /var/www/html,
        delay = 1,
        rsync = {
                archive = true,
                compress = true,
                whole_file = false
        },
        ssh = {
                port = 22
        }
}
```

Sur le routeur PfSense

Voici les 3 adresses IP de nos routeurs après les avoir configuré :



Et les 3 @MAC de nos routeurs après avoir configuré l'@IP

Adresse mac WAN 00:0C:29:CB:C7:67 ---→ em1

Adresse Mac de ma 1ère carte réseau (en lan) : 00:0C:29:CB:C7:5D ----->em0

Adresse mac DMZ 00:0C:29:CB:C7:71----->em2

Configuration BDD

Après avoir fait un « apt update » & « apt install mariadb-server »

On configure la carte réseau en LAN static

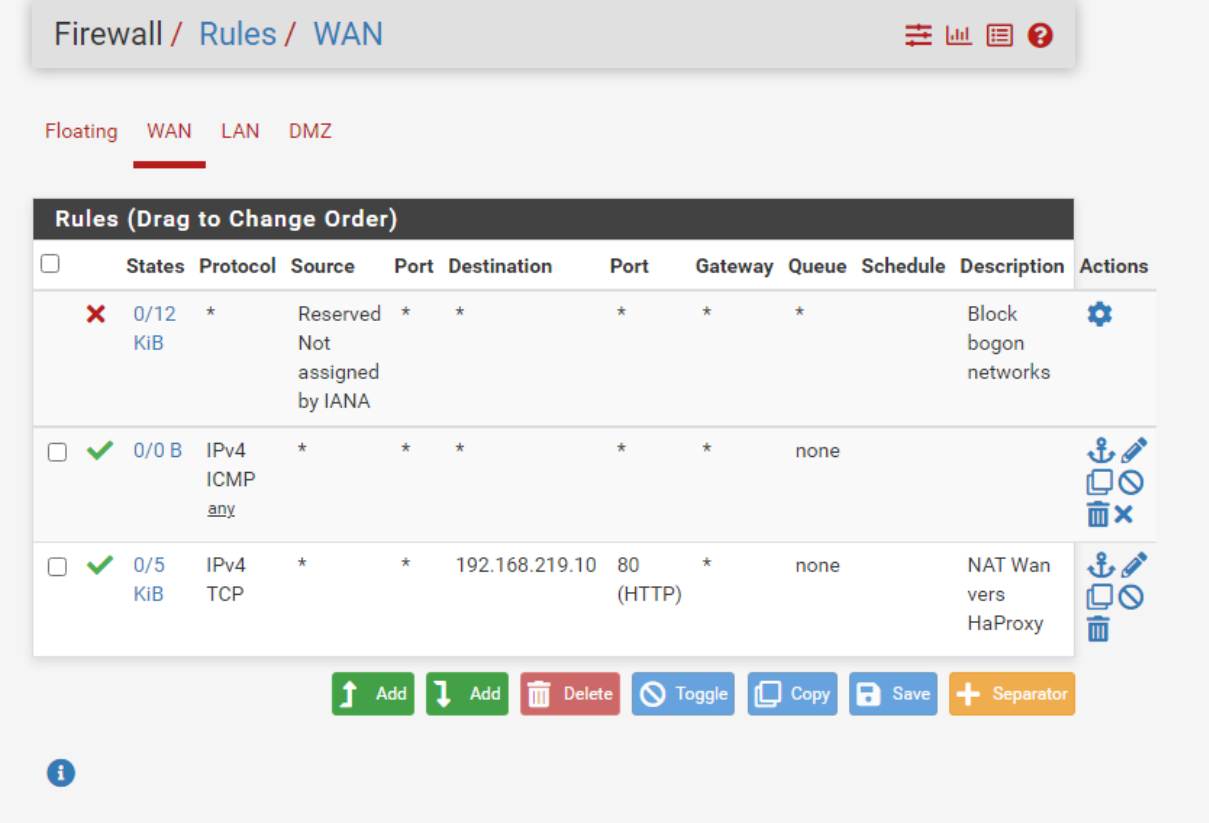
```
# The primary network interface
auto ens33
iface ens33 inet static
address 10.20.0.30/16

auto ens34
iface ens34 inet dhcp
```

```
MariaDB [haproxy]> INSERT INTO MEMBRE(login, mdp, nom, prenom) VALUES
    -> ('alves','123','Alves','Manuel'),
    -> ('thevenin','123','Thevenin','Olivier');
ERROR 1146 (42S02): Table 'haproxy.MEMBRE' doesn't exist
MariaDB [haproxy]> INSERT INTO membre(login, mdp, nom, prenom) VALUES ('alves','123','Alves','Manuel
'), ('thevenin','123','Thevenin','Olivier');
Query OK, 2 rows affected (0,001 sec)
Records: 2  Duplicates: 0  Warnings: 0

MariaDB [haproxy]> _
```

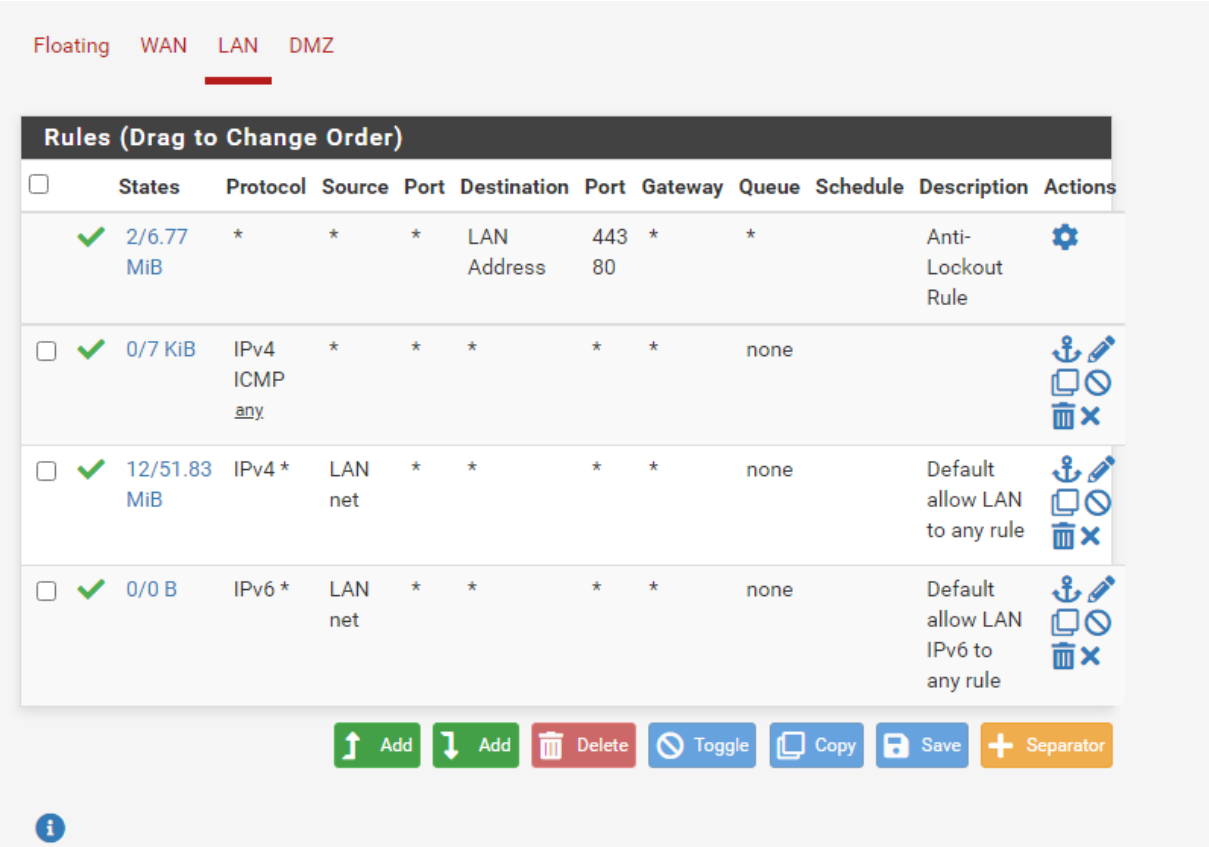
Comme demander sur le TP ont créé la base mariadb « HaProxy » dans laquelle on ajoute nos utilisateurs avec leurs login et leurs mdp

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| haproxy            |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0,029 sec)

MariaDB [(none)]> use haproxy
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [haproxy]> show tables;
+-------------------+
| Tables_in_haproxy |
+-------------------+
| membre            |
+-------------------+
1 row in set (0,000 sec)

MariaDB [haproxy]> use membre
ERROR 1049 (42000): Unknown database 'membre'
MariaDB [haproxy]> select * from membre
    -> ;
+----+----------+-----+----------+---------+
| id | login    | mdp | nom      | prenom  |
+----+----------+-----+----------+---------+
|  1 | alves    | 123 | Alves    | Manuel  |
|  2 | thevenin | 123 | Thevenin | Olivier |
+----+----------+-----+----------+---------+
2 rows in set (0,001 sec)
```

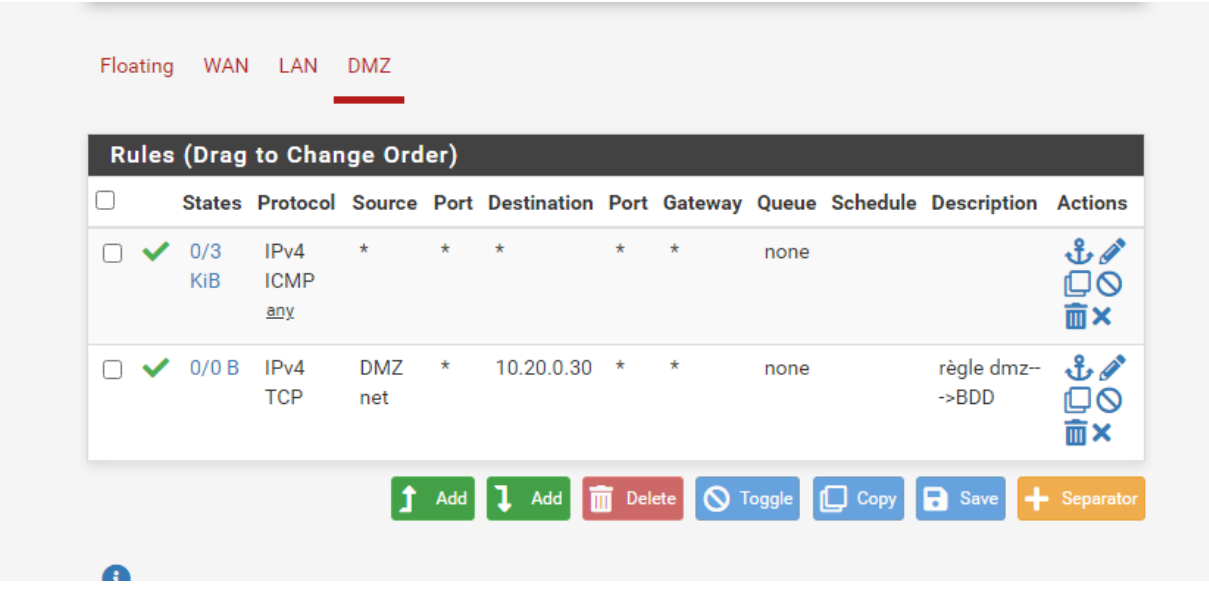
Règles PfSense



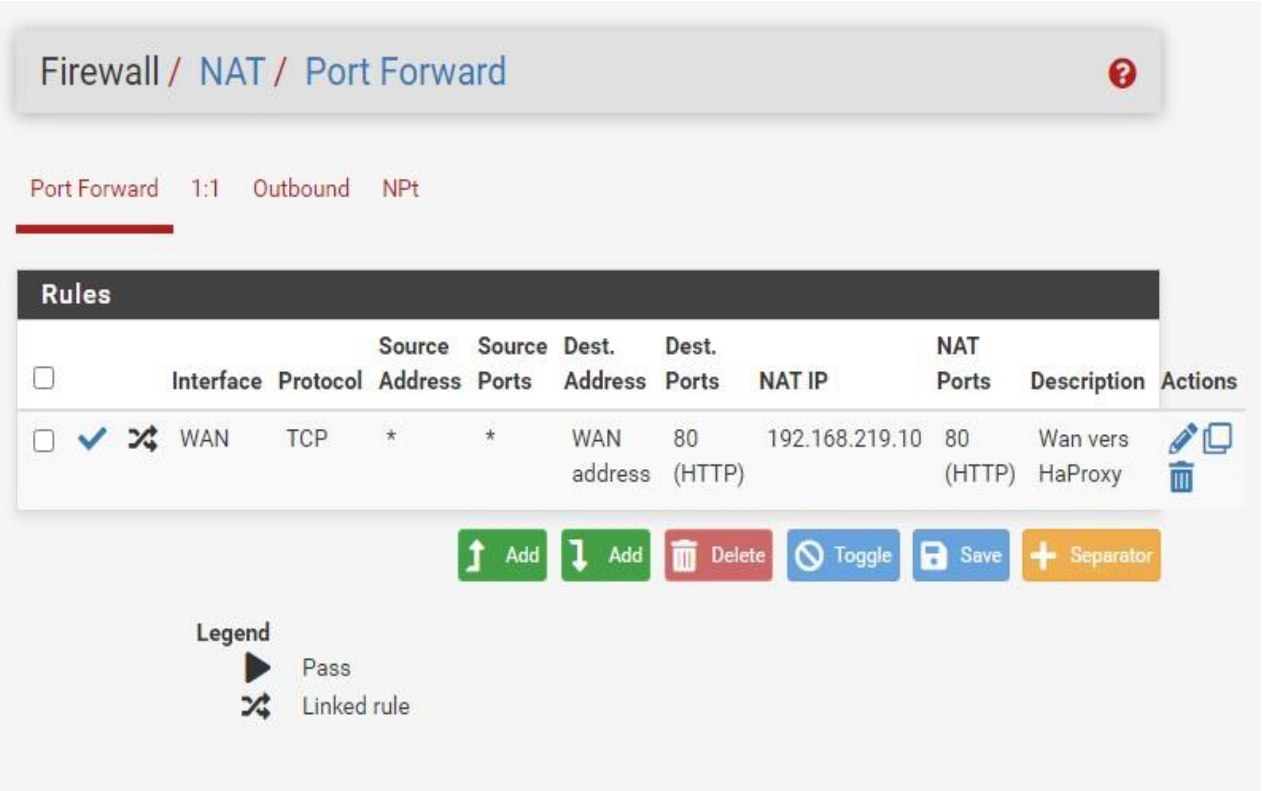
On paramètre nos règles afin d'autoriser les connexions à l'interface Web



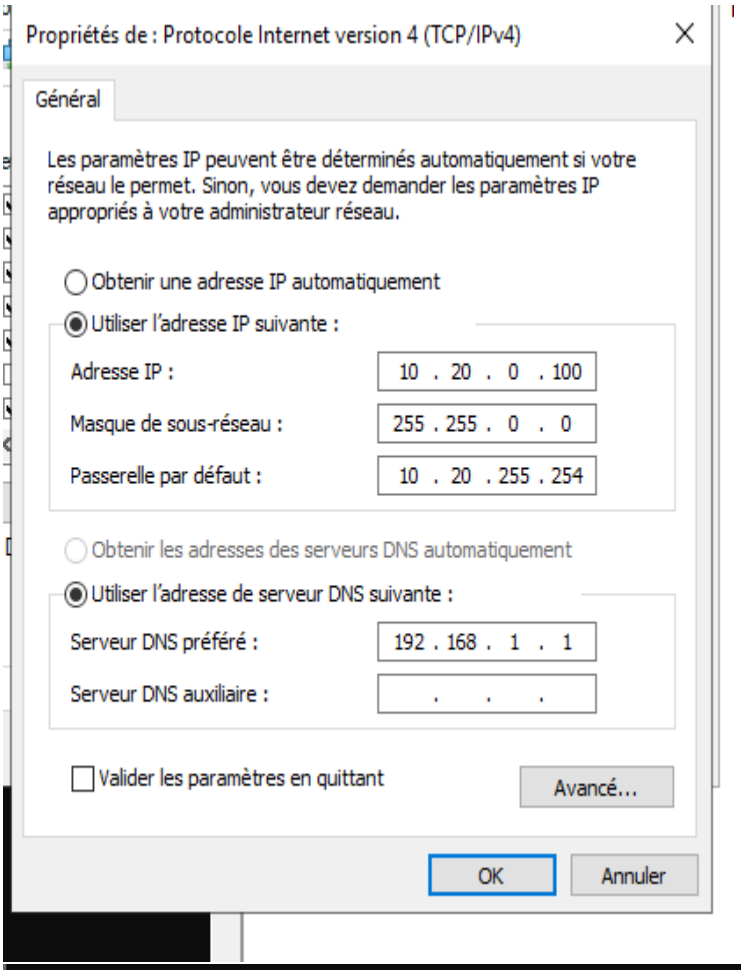
*on a fait des aliases sur les ports 443 et 80 (HTTPS / http), puis on a effectué des règles afin de filtrer le trafic entrant / sortant

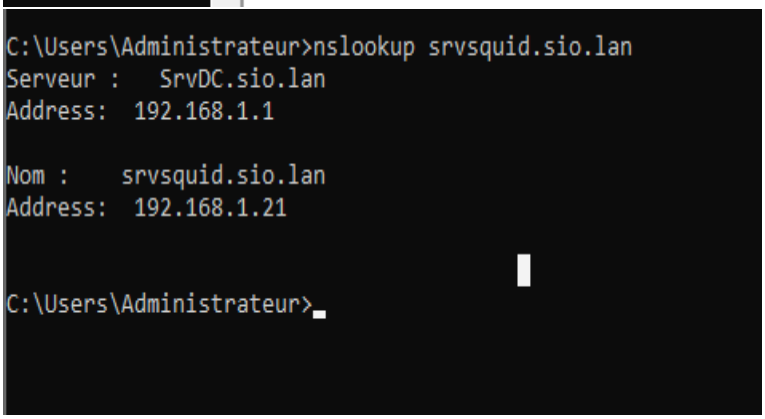


Et là on a configuré la DMZ de sortes à ce que la machine du réseau soit accessible depuis l'extérieur

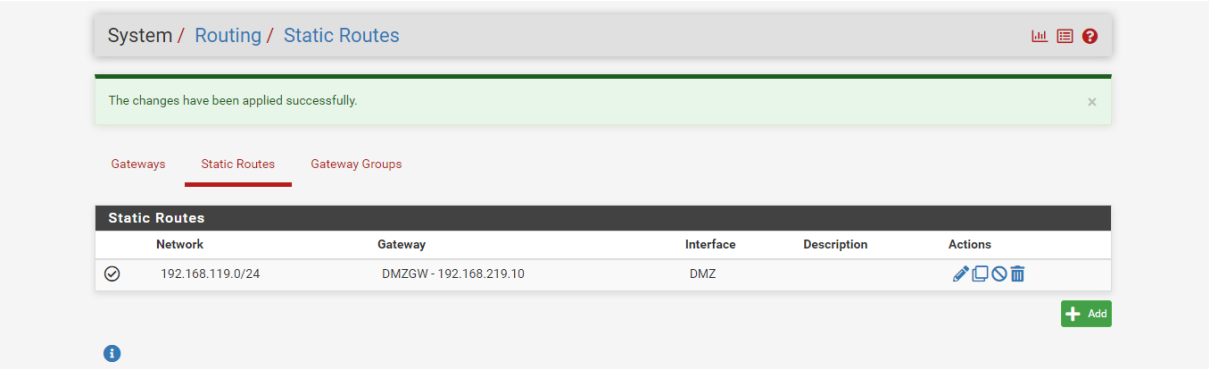


Et pour finir on effectue, une règle NAT qui effectue une redirection de ports





La machine est bien sur le réseau



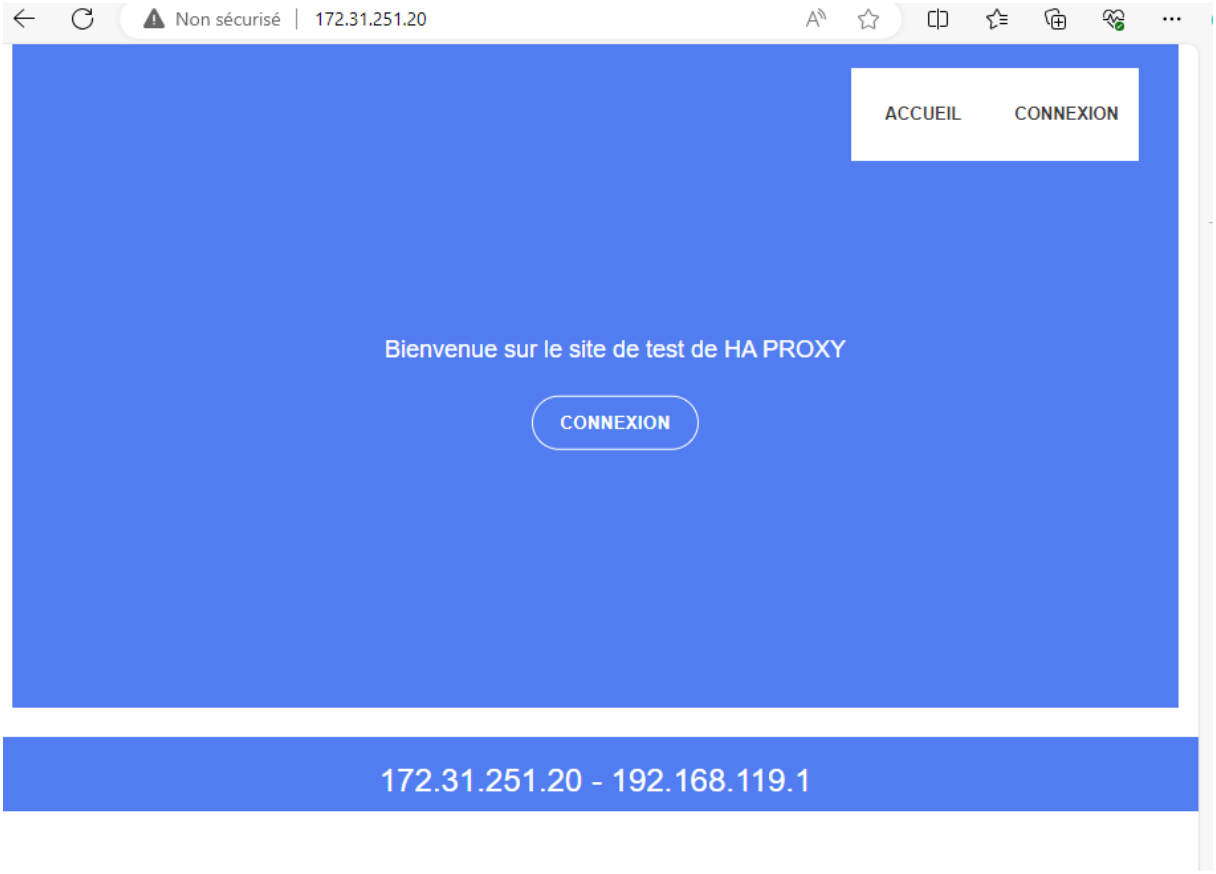
Ajout d'une route statique [car le Pfsense connaît que les 3 réseaux]

```
MariaDB [(none)]> use mysal
ERROR 1049 (42000): Unknown database 'mysal'
MariaDB [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]> USE
USE             USE_FRM         USER            USER_RESOURCES
MariaDB [mysql]> USE haproxy
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [haproxy]> GRANT ALL PRIVILEGES ON haproxy.* TO 'root'@'%' IDENTIFIED BY 'root' WITH GRANT O
PTION;
Query OK, 0 rows affected (0,002 sec)

MariaDB [haproxy]> flush privileges;
Query OK, 0 rows affected (0,001 sec)

MariaDB [haproxy]>
```

*attribution des droits à route pour accéder à l'HAPROXY

```
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
```

*Ouverture du port d'écoute pour tout le monde



On a bien accès à notre HaProxy !