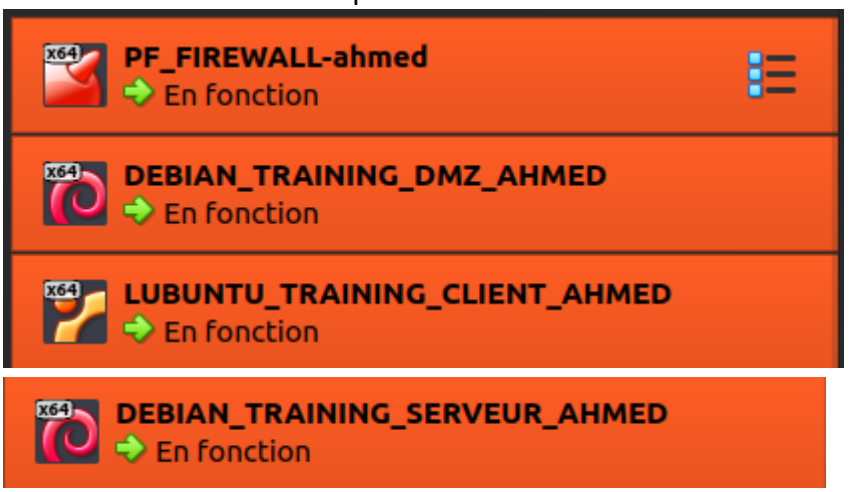
Labo FIREWALL

Je commence tout d'abord par lancé les machines essentiels à la réalisation du contexte :



2°) Prise en main du contexte

2.1°) Mise en place de la maquette de travail

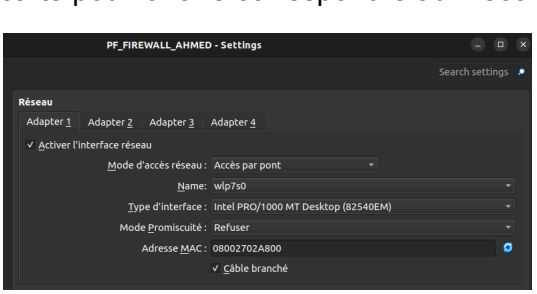
On doit tout d'abords commencer par effectuer les configurations réseaux afin de pouvoir faire communiquer les machines entre elles :

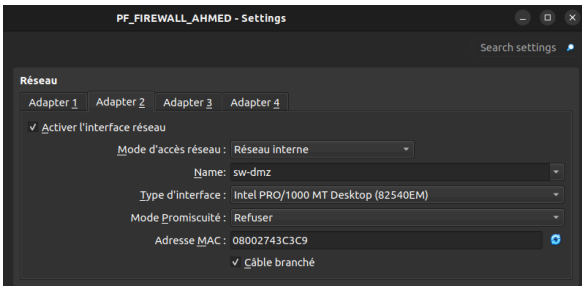
On commenceras tout d'abords par le parefeu :

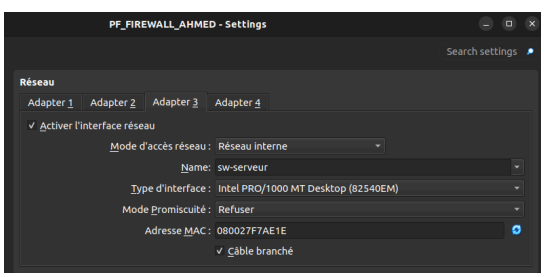
Machine PF_FIREWALL :

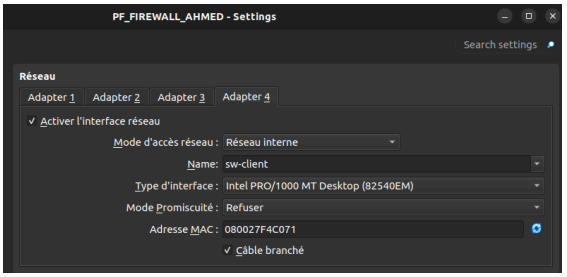
CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Accès par pont sur la carte filaire du réseau du lycée.
Interface 2 (à activer)	Réseau interne nommé sw-dmz.
Interface 3 (à activer)	Réseau interne nommé sw-serveur.
Interface 4 (à activer)	Réseau interne nommé sw-client.

on se rend alors dans configuration de virtualbox puis réseaux et on selectionne chaque carte pour la faire correspondre aux recommandations :





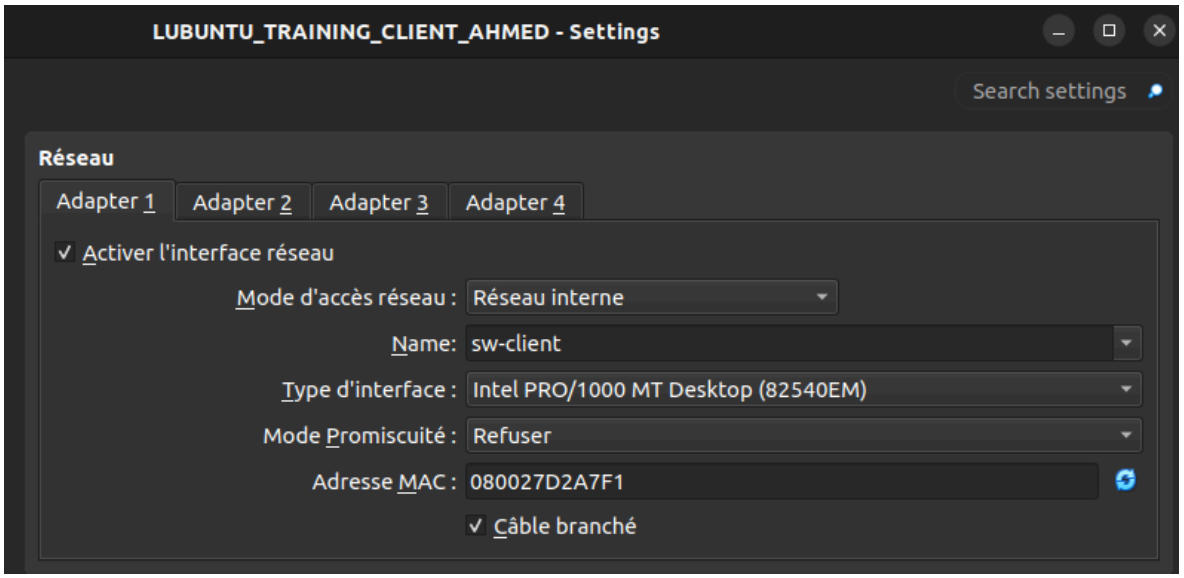




Faire la même chose pour le restant des machine :

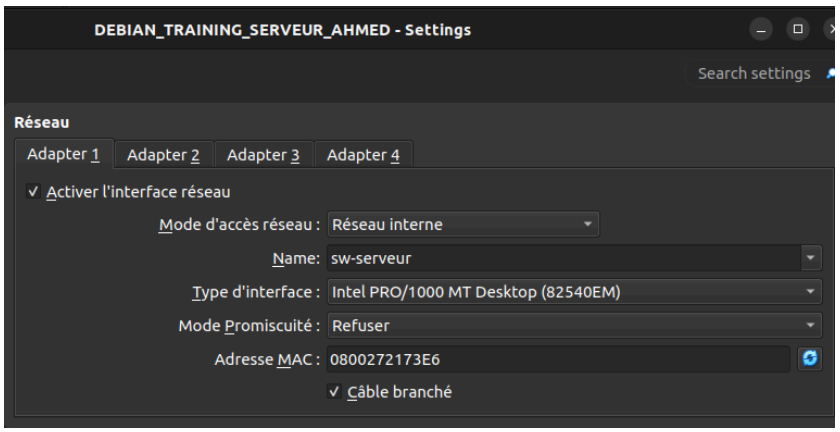
Machine DEBIAN_TRAINING_CLIENT :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Réseau interne nommé sw-client.



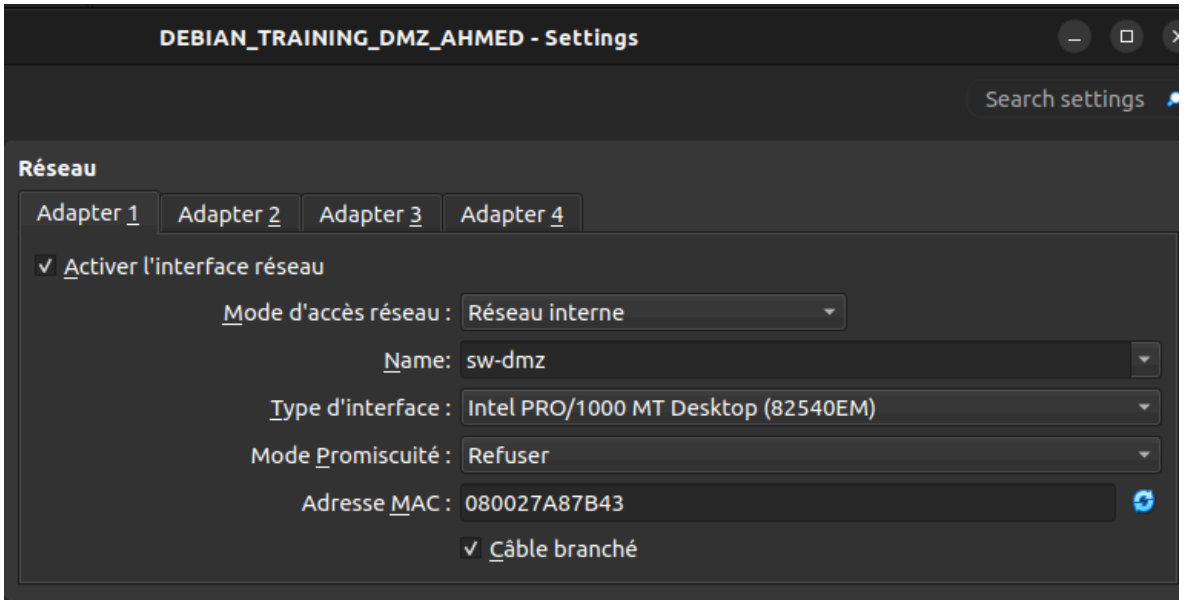
DEBIAN_TRAINING_SERVEUR :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Réseau interne nommé sw-serveur.



DEBIAN_TRAINING_DMZ :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Réseau interne nommé sw-dmz.



Ne pas oublier de re-générer les adresses MAC.

On doit ensuite modifier le serveur DNS afin de changer les forwarder. Pour cela lancer la machine **DEBIAN_TRAINING_SERVEUR :**

- **ouvrir le fichier /etc/bind/named.conf.options**
- **modifier la mention 8.8.8.8 par 172.16.10.20 et 172.16.10.21**
- **Sauvegarder le fichier**
- **Relancer le service bind9 avec la commande “systemctl restart bind9”**
- **Vérifier qu’il n’y as pas de soucis avec la commande “systemctl bind9 status”**

On obtient alors ce résultat :

```
 GNU nano 7.2                                          /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
           172.16.10.20;

           172.16.10.21;
        };
```

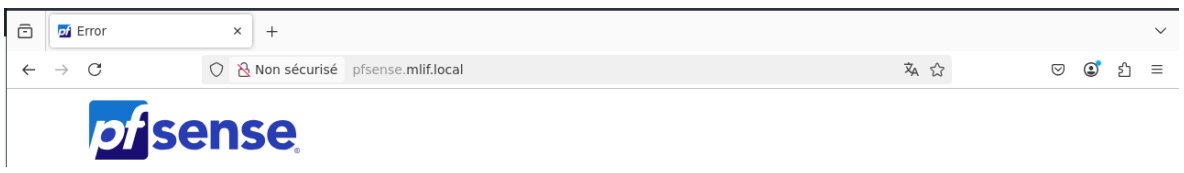
```
root@messagelab:~# systemctl restart bind9
root@messagelab:~# systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-11-23 17:11:22 CET; 6s ago
       Docs: man:named(8)
   Main PID: 1010 (named)
     Status: "running"
      Tasks: 4 (limit: 1097)
     Memory: 11.2M
        CPU: 22ms
     CGroup: /system.slice/named.service
             └─1010 /usr/sbin/named -f -u bind
```

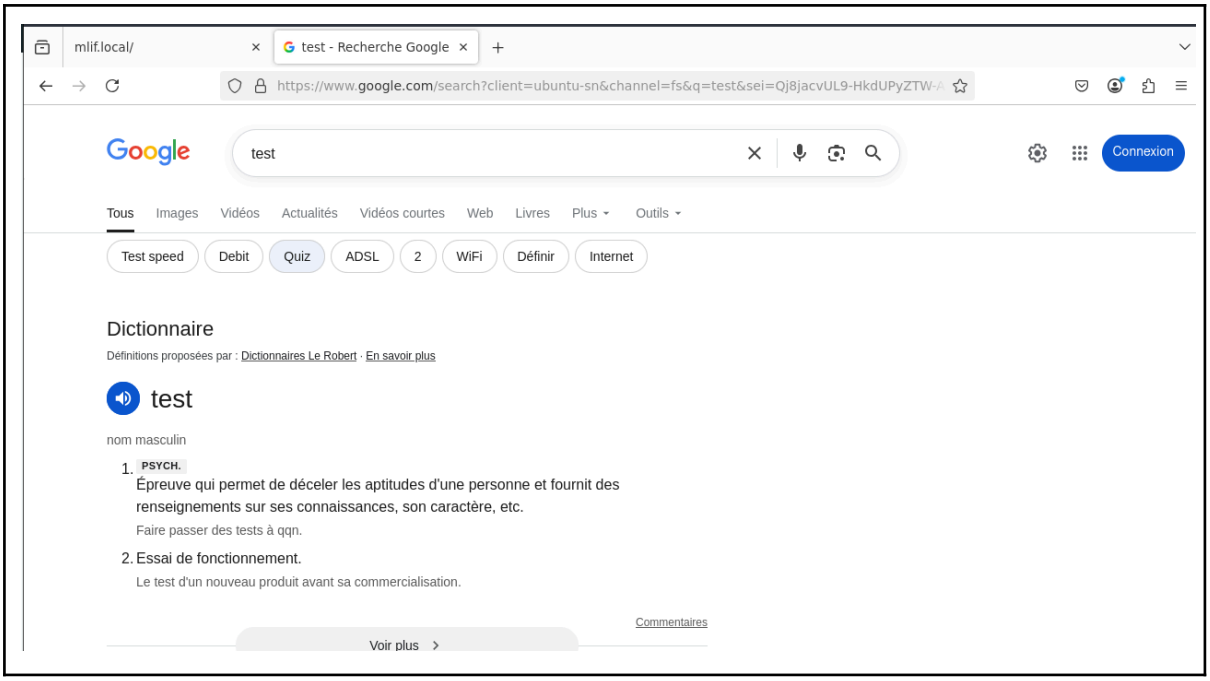
2.2°) Tests de prise en main de la maquette de travail

Passons maintenant au test de prise en main de la maquette de travail :

Depuis la machine DEBIAN_TRAINING_CLIENT, on ouvre le navigateur et on teste :

- un accès au serveur web en saisissant **www.mlif.local**,
- un accès au pare-feu en saisissant https://pfsense.mlif.local.
- Enfin on tester un accès à Internet en effectuant une recherche sur google





Depuis la machine DEBIAN_TRAINING_DMZ :

Tester les commandes suivantes :

- **ping messagelab.mlif.local**
- **nslookup www.mlif.local**
- **ping www.cisco.com**

```
root@www:~# ping messagelab.mlif.local
PING messagelab.mlif.local (192.168.100.10) 56(84) bytes of data.
64 bytes from messagelab.mlif.local (192.168.100.10): icmp_seq=1 ttl=63 time=0.264 ms
64 bytes from messagelab.mlif.local (192.168.100.10): icmp_seq=2 ttl=63 time=0.370 ms
64 bytes from messagelab.mlif.local (192.168.100.10): icmp_seq=3 ttl=63 time=0.339 ms
^C
--- messagelab.mlif.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.264/0.324/0.370/0.044 ms
root@www:~# nslookup www.mlif.local
Server:         192.168.100.10
Address:        192.168.100.10#53

Name:   www.mlif.local
Address: 192.168.200.5

root@www:~# ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (23.46.188.98) 56(84) bytes of data.
64 bytes from 23.46.188.98: icmp_seq=1 ttl=55 time=8.13 ms
64 bytes from 23.46.188.98: icmp_seq=2 ttl=55 time=6.44 ms
64 bytes from a23-46-188-98.deploy.static.akamaitechnologies.com (23.46.188.98): icmp_seq=3 ttl=55 time=59.6 ms
64 bytes from a23-46-188-98.deploy.static.akamaitechnologies.com (23.46.188.98): icmp_seq=4 ttl=55 time=20.9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6173ms
rtt min/avg/max/mdev = 6.436/23.754/59.561/21.415 ms
root@www:~#
```

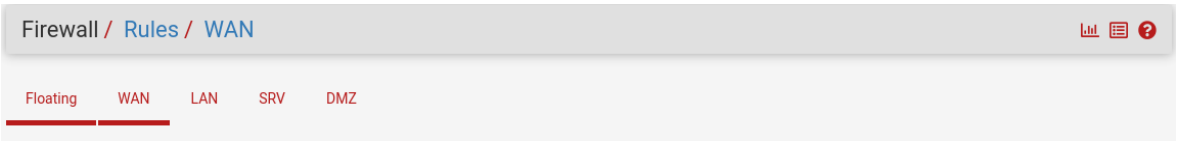
Les ping fonctionne bien et on voit bien que c'est le serveur dns qui réponds avec la présence de l'ip du dns lors du "nslookup", effectivement on y voit bien l'ip 192.168.100.10.

3°) Refus implicite (implicit deny)

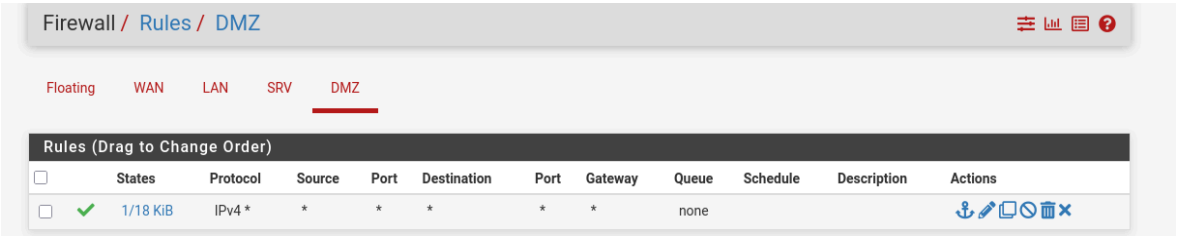
Depuis la machine client, on se connecte au pare-feu avec le compte **admin** et le mot de

passe **pfsense**.
Ensuite, on clique sur le menu **Firewall** puis sur **Rules**. On constate qu'il y a autant d'onglets que d'interfaces.

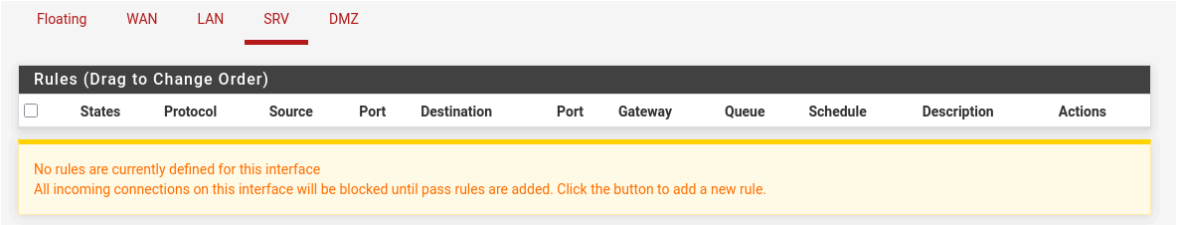
Ayant activé 4 interfaces lors des configurations du pare feu sur virtual box, c'est effectivement celles ci que l'on retrouve sur le "web configurator" de notre pare feu pfsense.



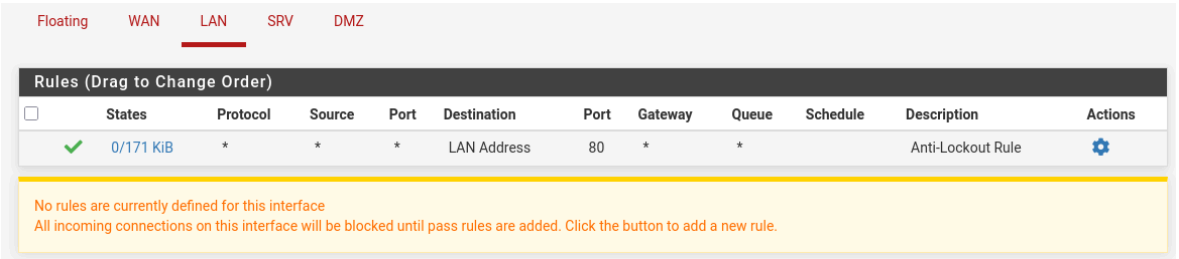
Cliquer sur l'interface DMZ et supprimer les deux dernière règles :



Cliquer ensuite sur l'interface SERVEURS et supprimer la dernière règle seulement :



Cliquer ensuite sur l'interface CLIENTS et faire de même en supprimant uniquement la dernière règle :



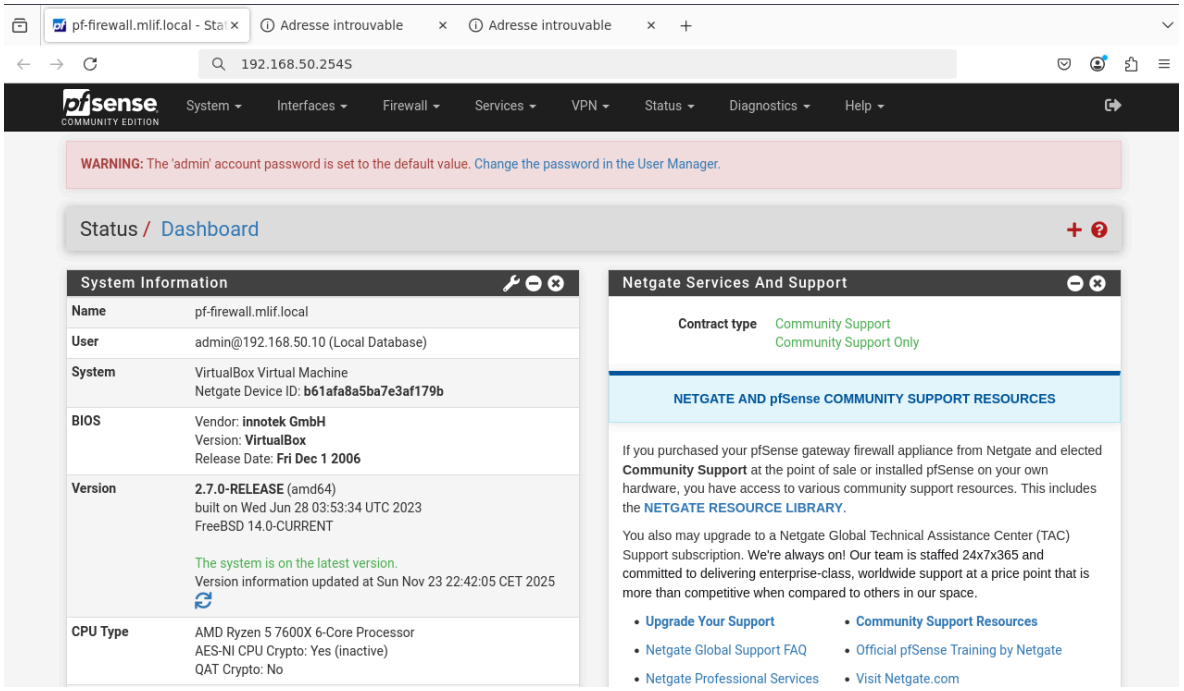
Depuis la machine DEBIAN_TRAINING_CLIENT :

étant donné que l'on est en train de mettre en place un implicit deny, on devrais avoir

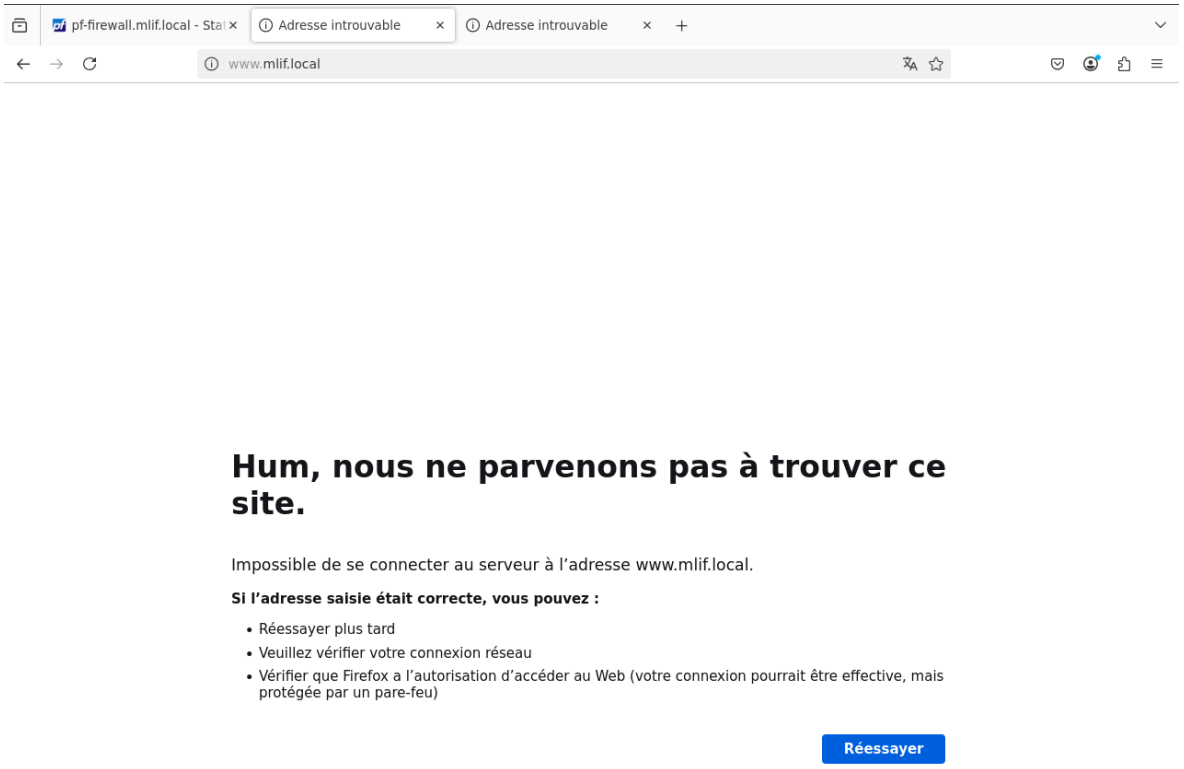
uniquement la page d'administration du pare-feu d'accessible. Ces pourquoi nous allons mener les tests suivant :

- vider le cache du navigateur pour être sûr que la recherche soit effectué et que ce ne soit pas le cache qui nous réponde.
- taper **https://192.168.50.254**, la recherche doit être réussie.
- taper www.mlif.local, la recherche doit échouer.
- faire une recherche quelconque, la recherche ne doit pas aboutir.

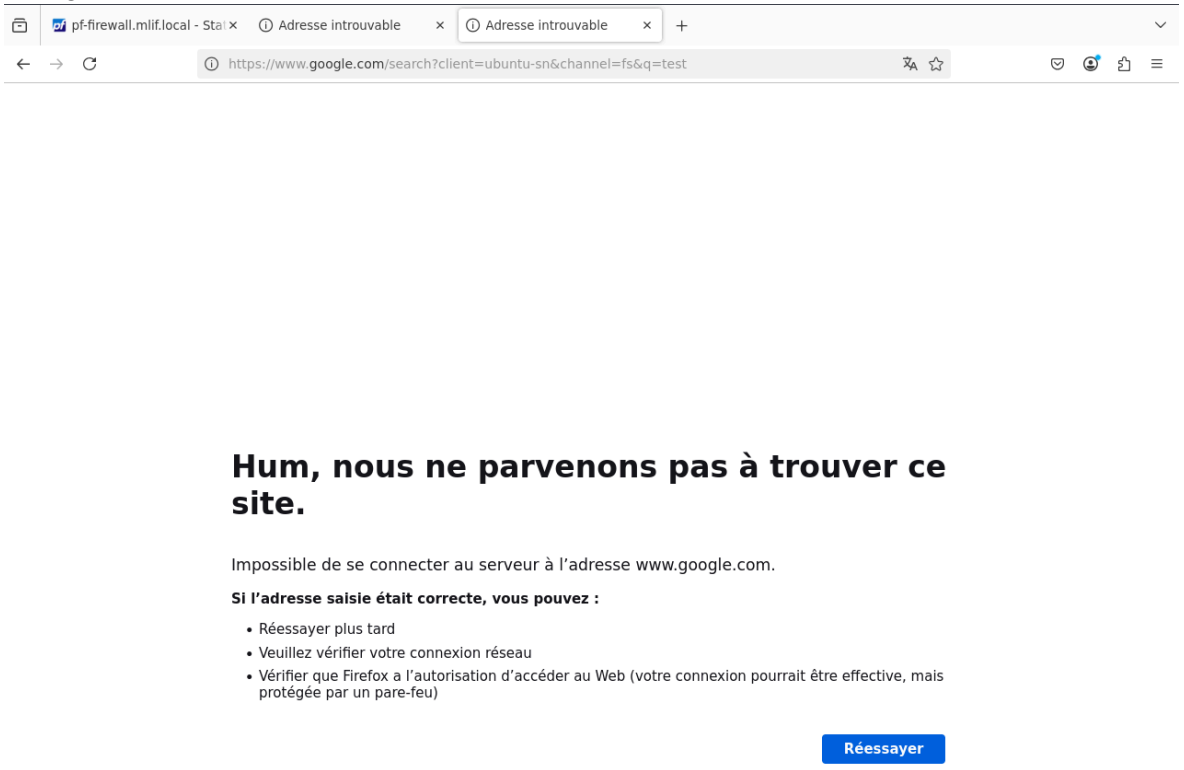
Résultat :



Le web configurator est toujours accessible. test réussi.



la page web mlif.local, la recherche n'abouti pas.



une recherche internet quelconque n'abouti pas.

On as bien réussi le début de notre implicit deny, effectivement seul les sites que l'on as autorisé sont accessible à savoir seul la page de configuration du pare feu.

Depuis la machine DEBIAN_TRAINING_DMZ :

Tester les commandes suivantes :

- ping messagelab.mlif.local
- ping www.cisco.com

```
root@www:~# ping www.cisco.com
ping: www.cisco.com: Échec temporaire dans la résolution du nom
root@www:~# ping messagelab.mlif.local
ping: messagelab.mlif.local: Échec temporaire dans la résolution du nom
```

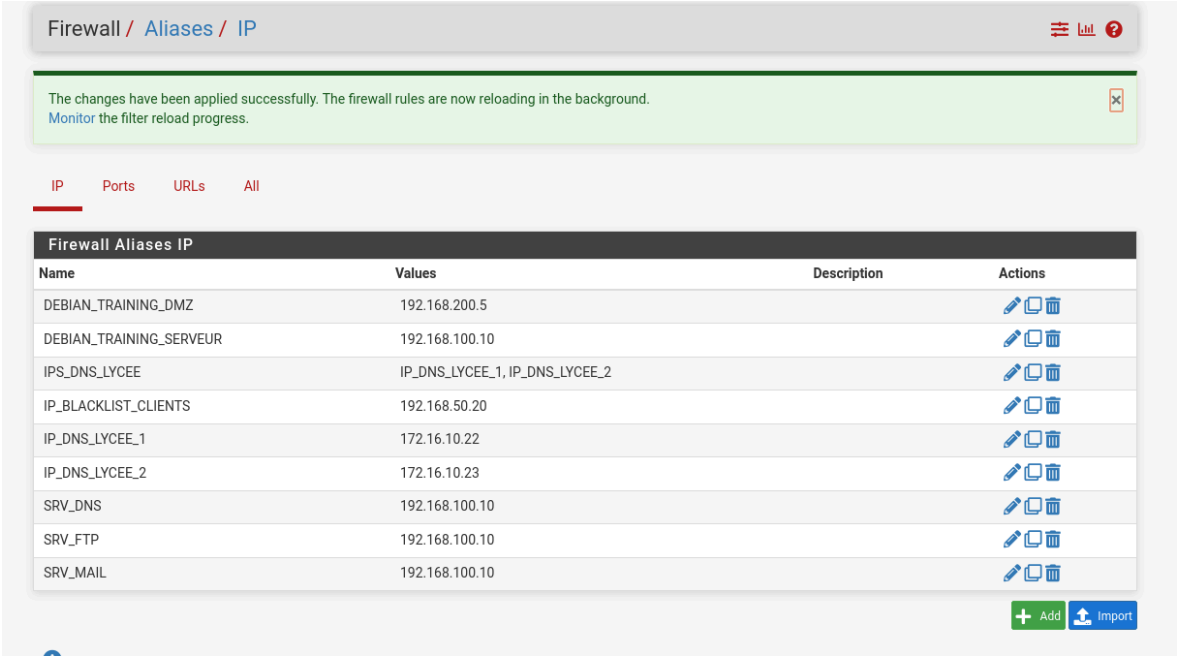
Les deux pings échouent c'est ce que l'on voulait.

On crée le snapshot

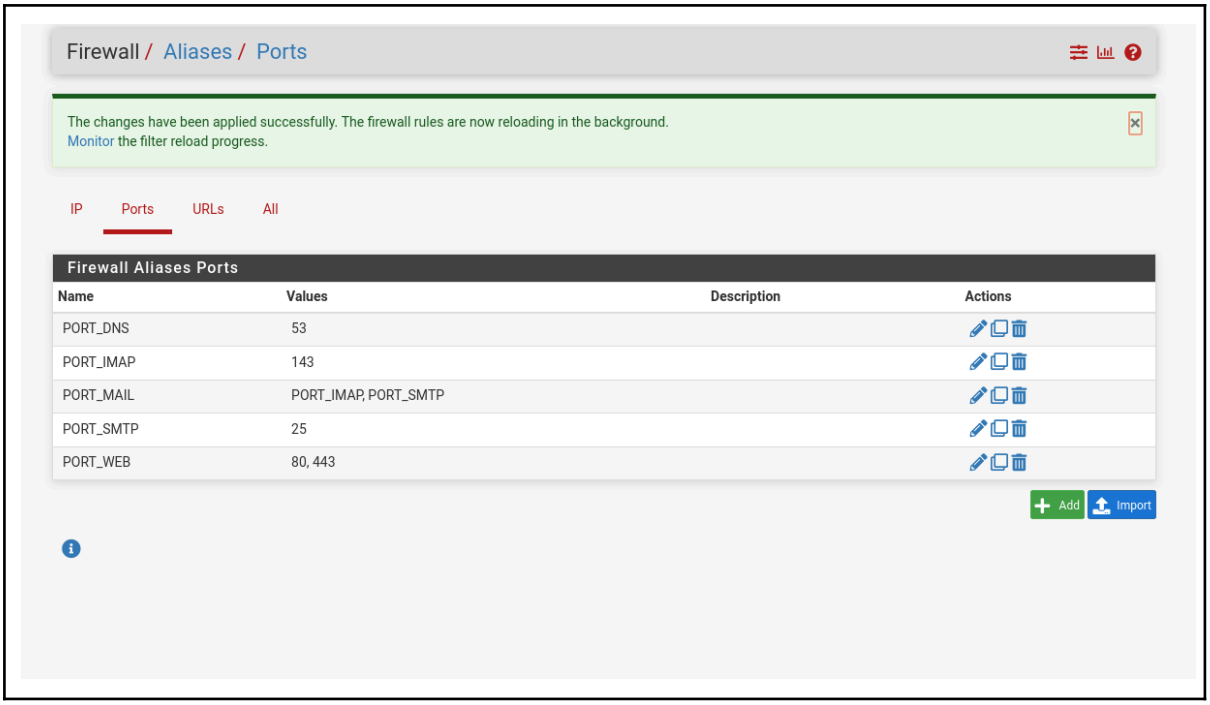
STOP 1 : Appelez moi pour que je puisse vérifier cette partie du travail.

4°) Création des aliases

Nous allons maintenant crée des aliases afin de la création et la maintenance des règles de filtrage et de NAT.
Pour ce faire nous allons nous rendre dans **Firewall** puis **Aliases.** Puis crée tout les aliases demandé :



les aliases ont été créés comme demandé, on passe au aliases de type **PORT:**

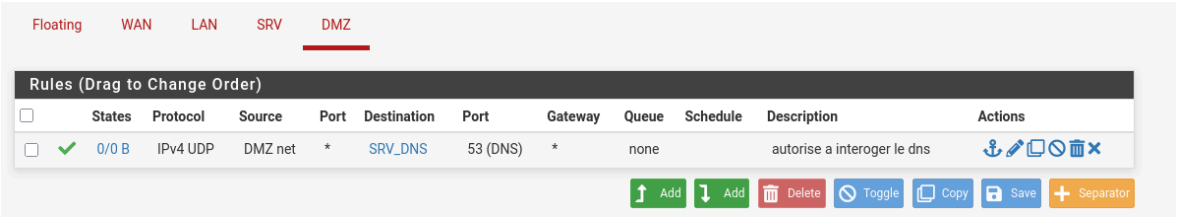


5°) Filtrage

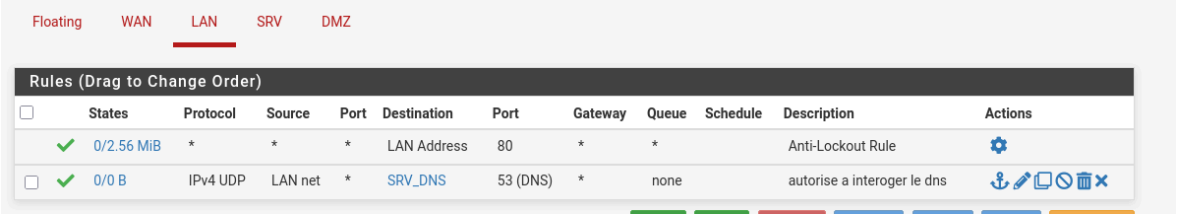
Nous allons maintenant configurer les règles de filtrage. Pour cela, nous nous rendons dans ***Firewall*** puis ***Rules***, et nous créons les règles dans les interfaces d'où provient le trafic, en utilisant au mieux les aliases définis précédemment.

Nous allons maintenant créer la règle R1. L'objectif est d'autoriser l'ensemble des machines des réseaux **DMZ**, **SERVEURS** et **CLIENTS** à i**nterroger le serveur DNS** du contexte, t**out en excluant l'adresse 192.168.50.20**. Pour cela, nous **utiliserons les aliases** des trois réseaux comme sources, l'alias **SRV_DNS en destination**, ainsi que le port **PORT_DNS**. Nous veillerons également à activer la journalisation et à placer la règle au bon endroit dans l'ordre de traitement.

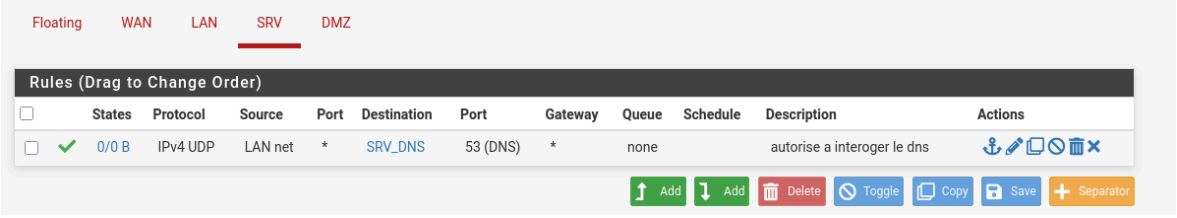
R1:
SUR DMZ :



SUR LAN (client) :



Sur SRV :



Vérification (depuis DEBIAN_TRAINING_CLIENT) :

Pour vérifier que le travail a bien été effectué on pense bien à vider le cache à l'aide de la commande **" resolvectl flush-caches ",** puis on utilise la commande :

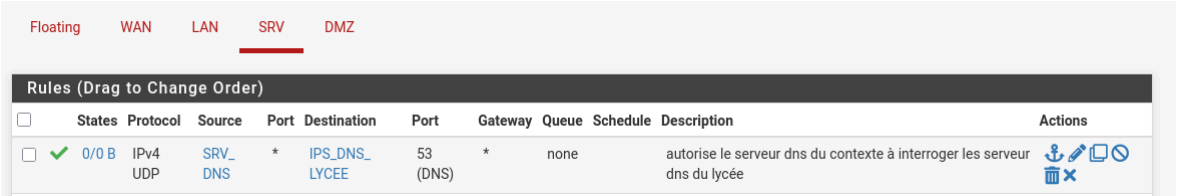
- nslookup www.mlif.local

```
test@client-mlif:~$ sudo resolvectl flush-caches
test@client-mlif:~$ nslookup www.mlif.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.mlif.local
Address: 192.168.200.5
```

R1 est bien validé.

R2:



R2 validé

R3 :
Sur SRV :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	0/0 B	IPv4 *	SRV_DNS	*	*	*	*	none		autorise SRV_DNS vers internet	
☐	0/0 B	IPv4 UDP	SRV_DNS	*	IPS_DNS_LYCEE	53 (DNS)	*	none		autorise le serveur dns du contexte à interroger les serveur dns du lycée	
☐	0/0 B	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		autorise a interoger le dns	

Add Add Delete Toggle Copy Save Separator

```
test@www:~$ nslookup free.fr
Server:         192.168.100.10
Address:        192.168.100.10#53

Non-authoritative answer:
Name:   free.fr
Address: 212.27.48.10
Name:   free.fr
Address: 2a01:e0c:1::1
```

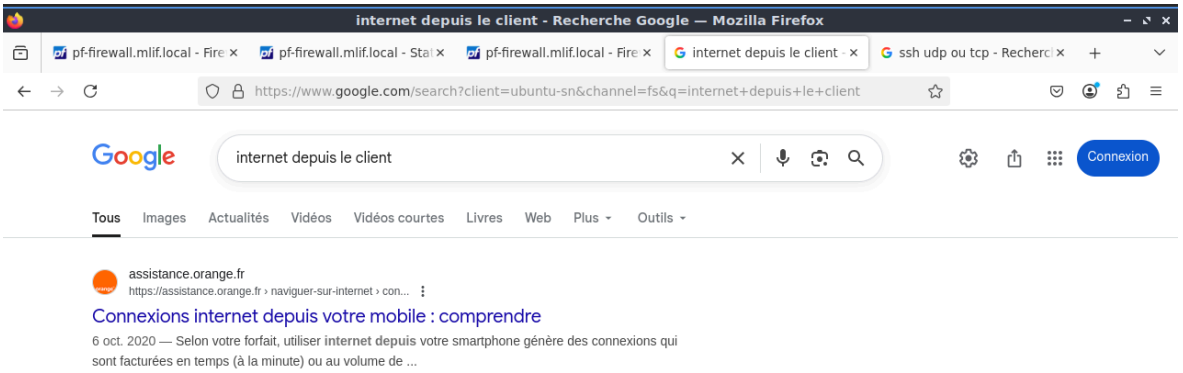
SUR LAN :

Floating WAN LAN SRV DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	1/2.78 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
☐	42/535 KiB	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		autorise a interoger le dns	
☐	61/2.75 MiB	IPv4 *	LAN net	*	*	*	*	none		autorise les clients a acceder a internet	

Add Add Delete Toggle Copy Save Separator



SUR DMZ :

Floating WAN LAN SRV DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	0/0 B	IPv4 *	DEBIAN_TRAINING_DMZ	*	*	*	*	none		autorise la dmz a sortir sur internet	
☐	0/5 KiB	IPv4 UDP	DMZ net	*	SRV_DNS	53 (DNS)	*	none		autorise a interoger le dns	

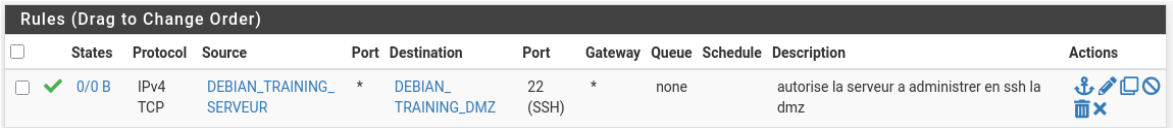
Add Add Delete Toggle Copy Save Separator

```
root@www:~# nslookup free.fr
Server:         192.168.100.10
Address:        192.168.100.10#53

Non-authoritative answer:
Name:   free.fr
Address: 212.27.48.10
Name:   free.fr
Address: 2a01:e0c:1::1
```

test réussi

R4 :
SUR SRV :



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✔ 0/0 B	IPv4 TCP	DEBIAN_TRAINING_SERVEUR	*	DEBIAN_TRAINING_DMZ	22 (SSH)	*	none		autorise la serveur a administrer en ssh la dmz	

```
root@messagelab:~# ssh test@www.mlif.local
The authenticity of host 'www.mlif.local (192.168.200.5)' can't be established.
ED25519 key fingerprint is SHA256:TwIqBeBni2hO+ApcaZi1I7DrRvOfiIctuhcqHFNRrp4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'www.mlif.local' (ED25519) to the list of known hosts.
test@www.mlif.local's password:
Linux www 6.1.0-33-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.133-1 (2025-04-10) 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.
Last login: Thu Apr 24 19:42:26 2025 from ::1
```

test réussi

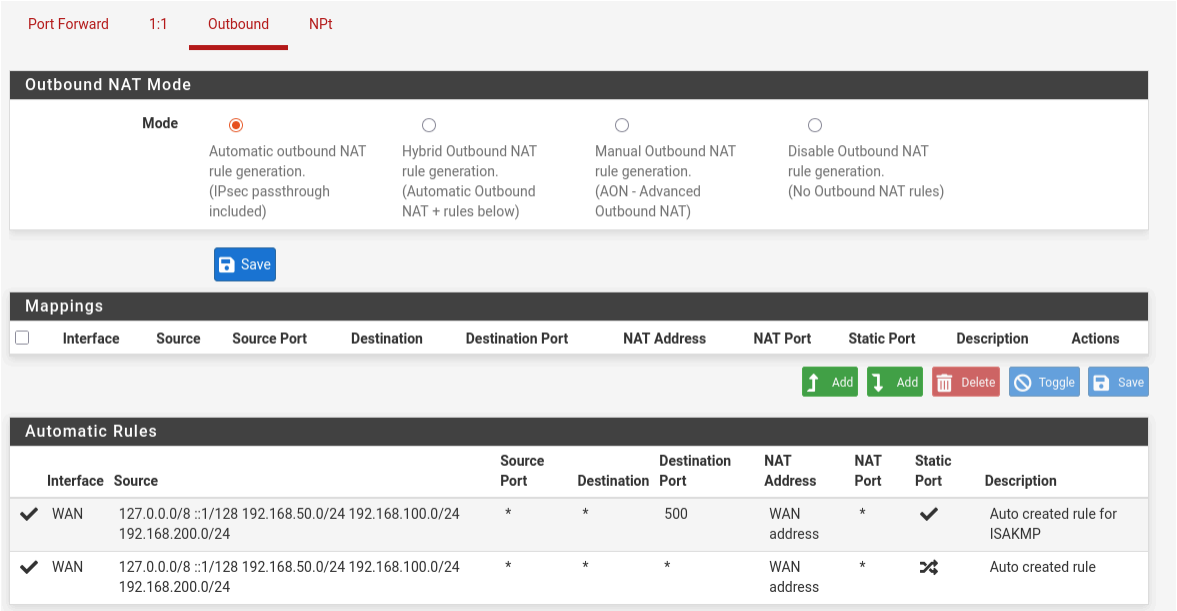
STOP 2 : Appelez moi pour que je puisse vérifier cette partie du travail.

6°) Traduction d'adresses

6.1°) Traduction des adresses sources

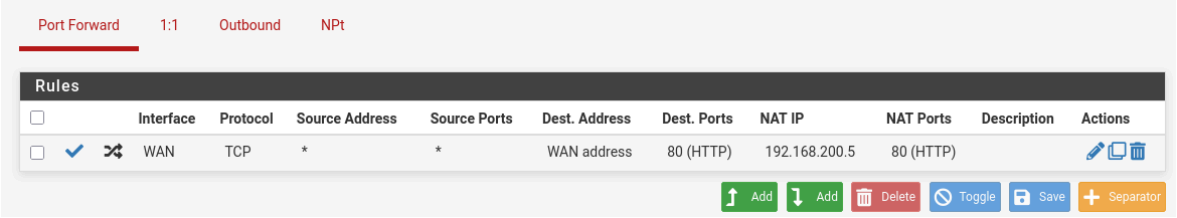
Nous allons maintenant vérifier la traduction d'adresses (NAT) utilisée par le pare-feu. Pour cela, nous nous rendons dans ***Firewall*** puis ***NAT***, et observons l'onglet ***Outbound***. Nous constatons que le mode automatique est déjà activé, ce qui signifie que pfsense gère lui-même la traduction des adresses privées vers l'extérieur. Aucune modification

n’est nécessaire dans le cadre de ce TP.

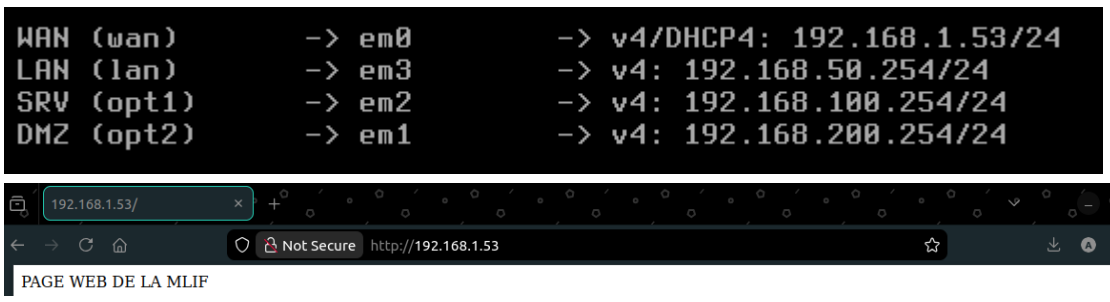


6.2°) Traduction des adresses de destination

Nous allons maintenant configurer une redirection de port afin de rendre le serveur web accessible depuis l’extérieur. Pour cela, nous nous rendons dans *Firewall* puis *NAT*, et ouvrons l’onglet ***Port Forward***. Nous y créerons une règle permettant aux machines du réseau externe (celui du lycée) d’atteindre le serveur web interne. Pour effectuer le test, nous utiliserons l’adresse WAN obtenue par DHCP. Comme pfsense bloque par défaut les flux RFC1918 vers l’interface WAN, nous retirerons provisoirement les deux règles correspondantes, puis nous vérifierons que la règle de filtrage associée au NAT a bien été ajoutée automatiquement.



Sur ma machine extérieure quand je tape l’adresse de l’adresse obtenue par dhcp j'obtiens bien la page web de la mlif donc c’est correcte.



STOP 3 : Appelez moi pour que je puisse vérifier cette partie du travail.