

## Labo FIREWALL

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



### 2°) Prise en main du contexte

#### 2.1°) Mise en place de la maquette de travail

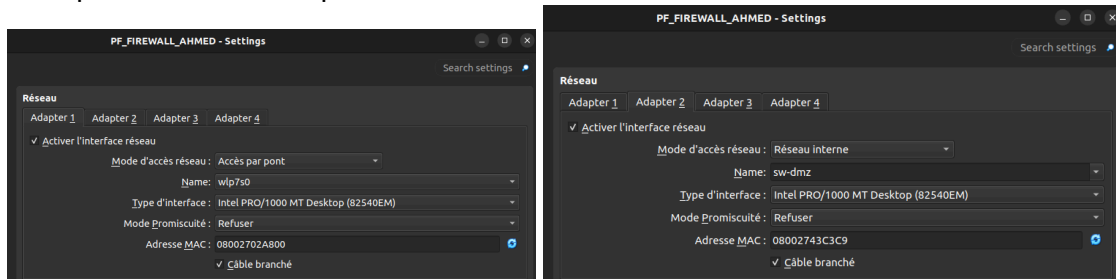
On doit tout d'abords commencer par effectuer les configurations réseaux afin de pouvoir faire communiquer les machines entre elles :

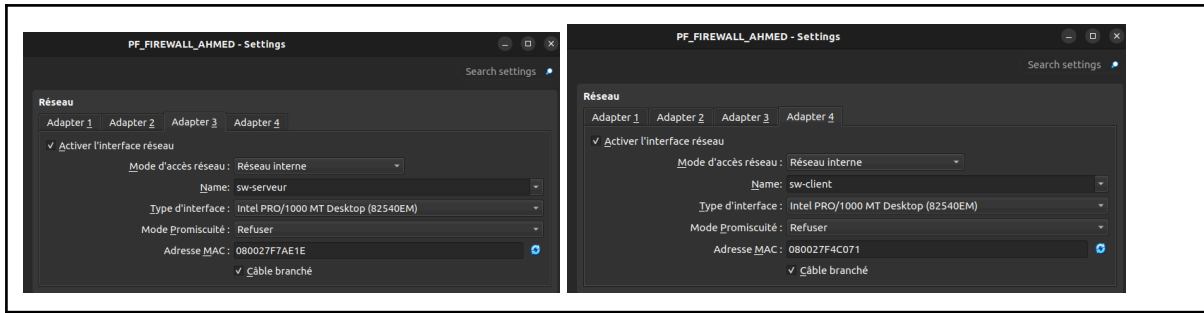
On commenceras tout d'abords par le parefeu :

#### **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 :

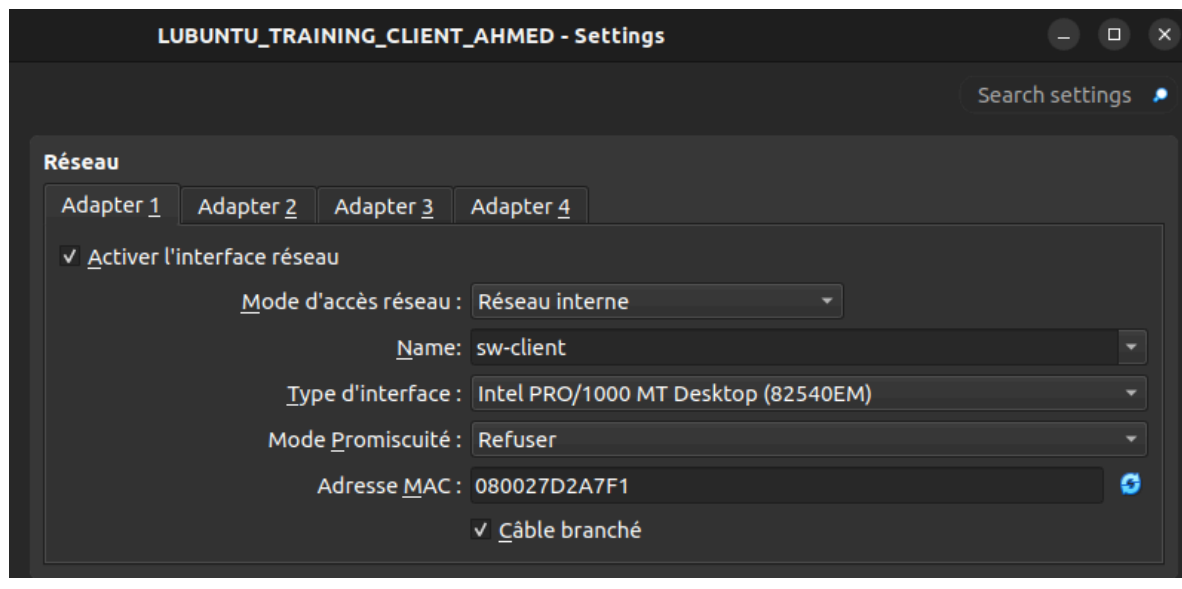




Faire la même chose pour le restant des machine :

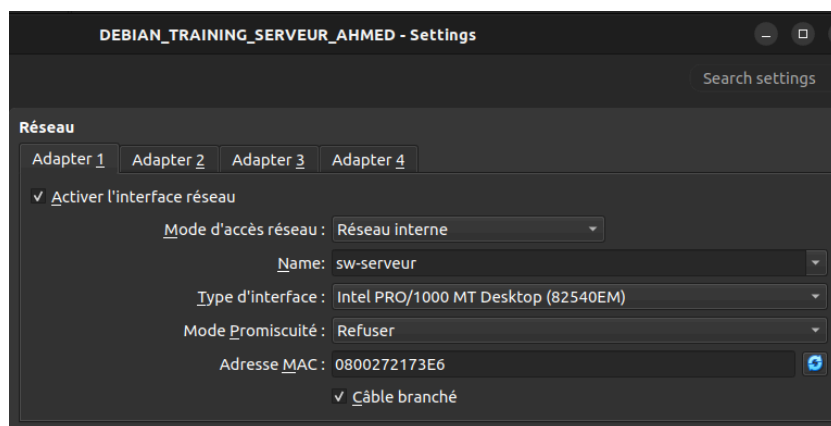
### Machine DEBIAN\_TRAINING\_CLIENT :

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



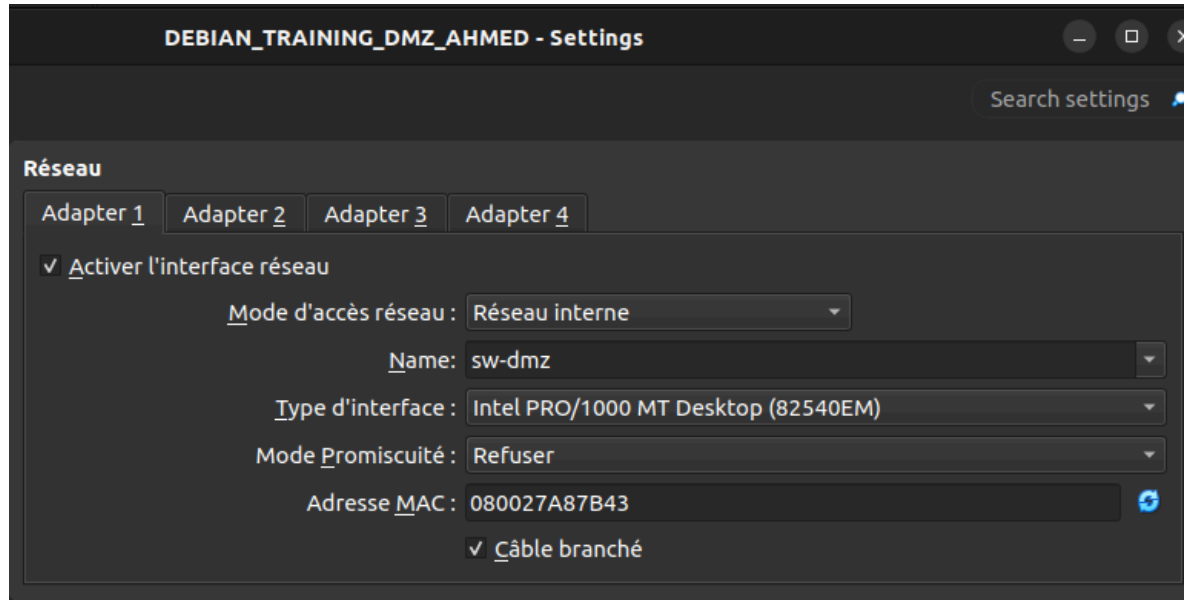
### DEBIAN\_TRAINING\_SERVEUR :

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 a 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;
    };
};

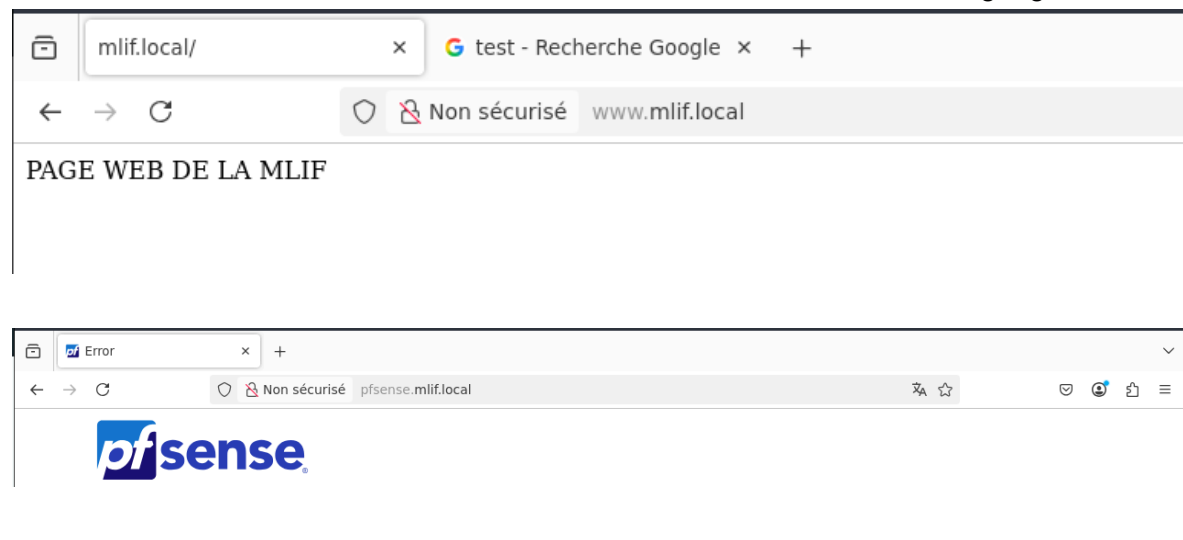
root@messagelab:~# systemctl restart bind9
root@messagelab:~# systemctl status bind9
• named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-11-23 17:11:22 CET; 6s ago
  Docs: man:named(8)
  Main 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
```

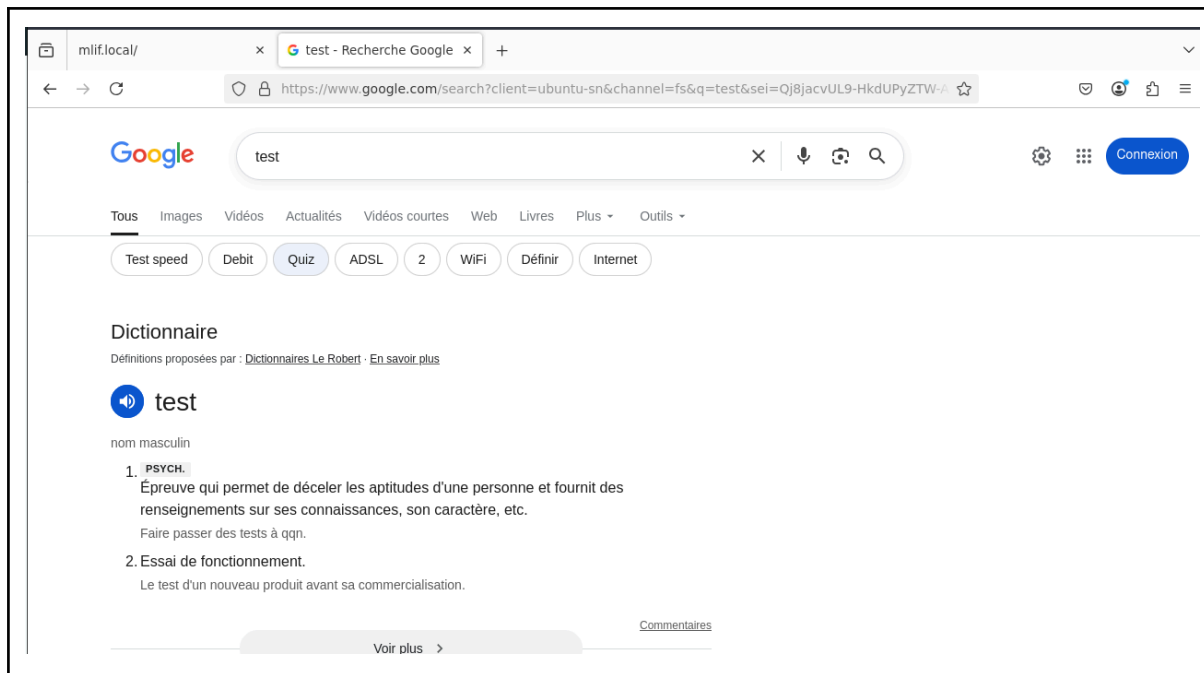
## 2.2°) Tests de prise en main de la maquette de travail

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](http://www.mlif.local),
- un accès au pare-feu en saisissant <https://pfsense.mlif.local>.
- Enfin on teste 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=0.13 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.

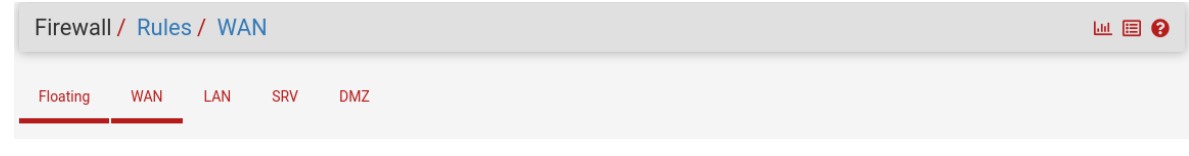
### 3°) Refus implicite (implicit deny)

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

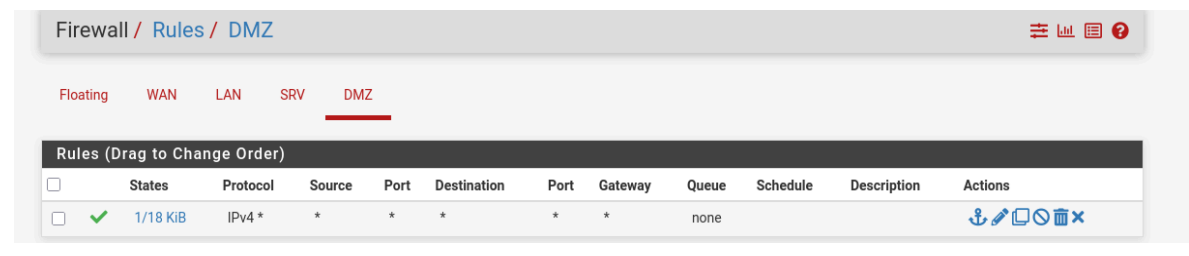
passer **pfSense**.

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

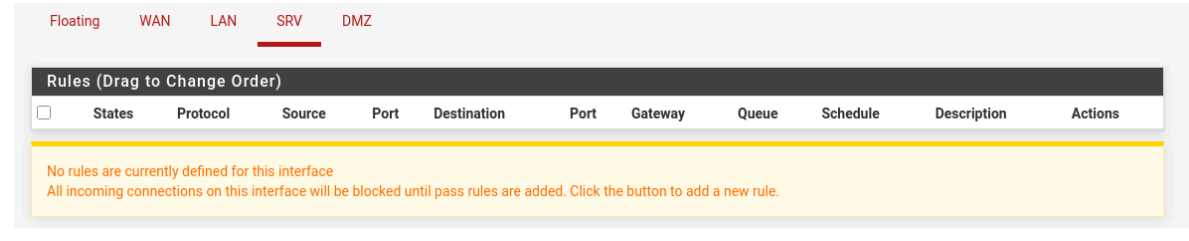
Ayant activé 4 interfaces lors des configurations du pare feu sur virtual box, c'est effectivement celles ci que l'on retrouve sur le "web configurator" de notre pare feu pfSense.



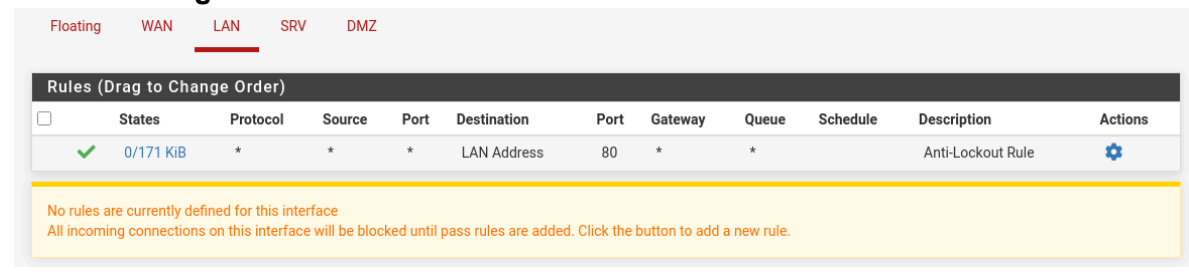
**Cliquer sur l'interface DMZ et supprimer les deux dernière règles :**



**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 devrait 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 effectuée 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](http://www.mlif.local), la recherche doit échouer.
- faire une recherche quelconque, la recherche ne doit pas aboutir.

## Résultat :

The screenshot shows the pfSense web configurator interface. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / Dashboard" section is visible. It contains two main panels: "System Information" and "Netgate Services And Support".

System Information	
Name	pf-firewall.mlif.local
User	admin@192.168.50.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: b61afa8a5ba7e3af179b
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT  The system is on the latest version. Version information updated at Sun Nov 23 22:42:05 CET 2025
CPU Type	AMD Ryzen 5 7600X 6-Core Processor AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

**Netgate Services And Support**

Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

Le web configurator est toujours accessible. test réussi.

The screenshot shows a Firefox browser window with three tabs: 'pf-firewall.mlif.local - Sta...', 'Adresse introuvable', and another 'Adresse introuvable'. The address bar contains 'www.mlif.local'. The main content area displays a large heading: **Hum, nous ne parvenons pas à trouver ce site.** Below this, it states: 'Impossible de se connecter au serveur à l'adresse www.mlif.local.' A sub-heading reads: 'Si l'adresse saisie était correcte, vous pouvez :'. This is followed by a bulleted list: 'Réessayer plus tard', 'Veuillez vérifier votre connexion réseau', and 'Vérifier que Firefox a l'autorisation d'accéder au Web (votre connexion pourrait être effective, mais protégée par un pare-feu)'. A blue 'Réessayer' button is positioned at the bottom right of the error message.

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

The screenshot shows a Firefox browser window with three tabs: 'pf-firewall.mlif.local - Sta...', 'Adresse introuvable', and another 'Adresse introuvable'. The address bar contains 'https://www.google.com/search?client=ubuntu-sn&channel=fs&q=test'. The main content area displays a large heading: **Hum, nous ne parvenons pas à trouver ce site.** Below this, it states: 'Impossible de se connecter au serveur à l'adresse www.google.com.' A sub-heading reads: 'Si l'adresse saisie était correcte, vous pouvez :'. This is followed by a bulleted list: 'Réessayer plus tard', 'Veuillez vérifier votre connexion réseau', and 'Vérifier que Firefox a l'autorisation d'accéder au Web (votre connexion pourrait être effective, mais protégée par un pare-feu)'. A blue 'Réessayer' button is positioned at the bottom right of the error message.

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](http://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 créer 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 créer tous les aliases demandés :

A screenshot of the Mikrotik WinBox Firewall Aliases IP configuration page. The breadcrumb navigation shows 'Firewall / Aliases / IP'. A green notification bar at the top states: 'The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.' Below this, there are tabs for 'IP', 'Ports', 'URLs', and 'All', with 'IP' selected. The main content is a table titled 'Firewall Aliases IP' with columns for Name, Values, Description, and Actions. The table lists several aliases with their respective IP addresses or ranges. At the bottom right, there are buttons for '+ Add' and 'Import'.

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

Firewall / Aliases / Ports

The changes have been applied successfully. The firewall rules are now reloading in the background.  
Monitor the filter reload progress.

IP **Ports** URLs All

Name	Values	Description	Actions
PORT_DNS	53		
PORT_IMAP	143		
PORT_MAIL	PORT_IMAP, PORT_SMTP		
PORT_SMTP	25		
PORT_WEB	80, 443		

Add Import

## 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 alias 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 **interroger le serveur DNS** du contexte, **tout en excluant l'adresse 192.168.50.20**. Pour cela, nous **utiliserons les alias** 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 :

Floating WAN LAN SRV **DMZ**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	DMZ net	*	SRV_DNS	53 (DNS)	*	none	autorise a interroger le dns	

Add Add Delete Toggle Copy Save Separator

### SUR LAN (client) :

Floating WAN LAN SRV DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/2.56 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 0/0 B	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		autorise a interoger le dns	

**Sur SRV :**

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 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		autorise a interoger le dns	

Add 
 Add 
 Delete 
 Toggle 
 Copy 
 Save 
 Separator

**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](http://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:**

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 UDP	SRV_DNS	*	IPS_DNS_LYCEE	53 (DNS)	*	none		autorise le serveur dns du contexte à interroger les serveur dns du lycée	

**R2 validé**

**R3 :  
Sur SRV :**

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	SRV_DNS	*	*	*	*	none		autorise SRV_DNS vers internet	
<input type="checkbox"/>	✓ 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	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		autorise a interroger 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)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/2.78 MIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 42/535 KiB	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		autorise a interroger le dns	
<input type="checkbox"/>	✓ 61/2.75 MIB	IPv4 *	LAN net	*	*	*	*	none		autorise les clients a acceder a internet	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

internet depuis le client - Recherche Google — Mozilla Firefox

[pf-firewall.mlif.local - Fire](#)
[pf-firewall.mlif.local - Sta](#)
[pf-firewall.mlif.local - Fire](#)
[internet depuis le client](#)
[ssh udp ou tcp - Recher](#)

<https://www.google.com/search?client=ubuntu-sn&channel=fs&q=internet+depuis+le+client>

Google

Tous Images Actualités Vidéos Vidéos courtes Livres Web Plus Outils

assistance.orange.fr  
<https://assistance.orange.fr/naviguer-sur-internet/comprendre>

**Connexions internet depuis votre mobile : comprendre**  
 6 oct. 2020 — Selon votre forfait, utiliser internet depuis votre smartphone génère des connexions qui sont facturées en temps (à la minute) ou au volume de ...

### SUR DMZ :

Floating WAN LAN SRV DMZ

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	DEBIAN_TRAINING_DMZ	*	*	*	*	none		autorise la dmz a sortir sur internet	
<input type="checkbox"/>	✓ 0/5 KiB	IPv4 UDP	DMZ net	*	SRV_DNS	53 (DNS)	*	none		autorise a interroger 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)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 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:TwIqBeBni2h0+ApcaZi1I7DrRv0fiIctuqcqHFNRrp4.
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.

Port Forward 1:1 **Outbound** NPT

**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)

**Mappings**

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

**Automatic Rules**

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8 ::1/128 192.168.200.0/24	192.168.50.0/24 192.168.100.0/24	*	*	500	WAN address	* <input checked="" type="checkbox"/> Auto created rule for ISAKMP
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8 ::1/128 192.168.200.0/24	192.168.50.0/24 192.168.100.0/24	*	*	*	WAN address	* <input checked="" type="checkbox"/> Auto created rule

## 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 créons 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.

Port Forward 1:1 **Outbound** NPT

**Rules**

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.200.5	80 (HTTP)

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.

```

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.53/24
LAN (lan)      -> em3      -> v4: 192.168.50.254/24
SRV (opt1)    -> em2      -> v4: 192.168.100.254/24
DMZ (opt2)    -> em1      -> v4: 192.168.200.254/24
  
```

192.168.1.53/

Not Secure http://192.168.1.53

PAGE WEB DE LA MLIF



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