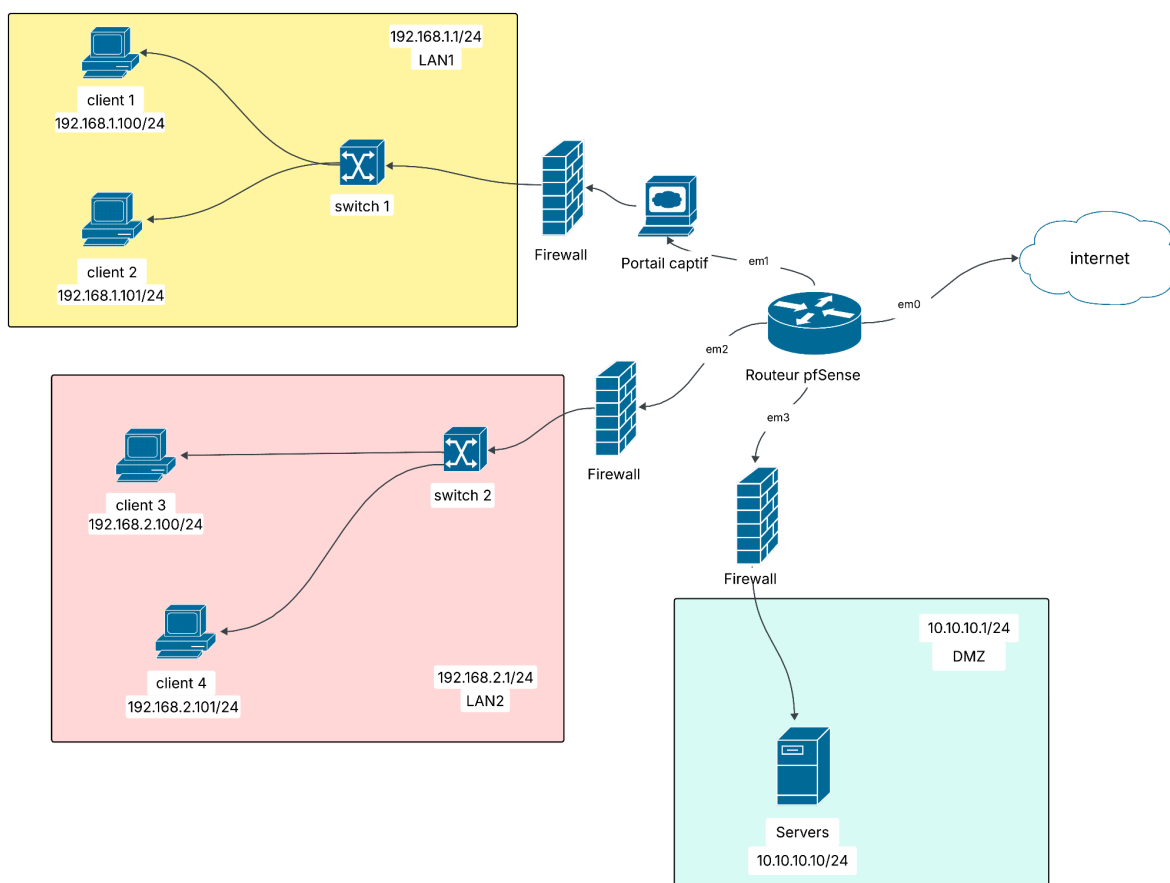


# Document d'architecture

## I. Schéma du réseau

Le réseau est structuré en trois zones distinctes, toutes interconnectées via une machine virtuelle pfSense, qui joue le rôle de routeur et de pare-feu. Le NAT est configuré sur l'interface WAN pour permettre aux machines internes d'accéder à Internet, tout en masquant leurs adresses IP privées. La première zone, LAN1, est dédiée aux invités et comprend deux machines virtuelles Ubuntu (client1 et client2). Son accès est limité à Internet via un portail captif, garantissant un contrôle strict des connexions. La deuxième zone, LAN2, représente le réseau interne d'une petite entreprise et abrite également deux machines virtuelles Ubuntu (client3 et client4). Contrairement à LAN1, elle dispose d'un accès complet à Internet et à la DMZ, permettant une communication fluide tout en maintenant une séparation sécurisée. Enfin, la DMZ comprend une seule machine virtuelle Ubuntu, dédiée à l'hébergement des serveurs. Bien qu'elle puisse se connecter à Internet, elle est isolée des réseaux LAN1 et LAN2 afin de limiter les risques en cas de cyberattaque.



## II. Plan d'adressage IP

| Interface | Port | Passerelle     | Plage DHCP                             | Rôle                 |
|-----------|------|----------------|--|----------------------|
| WAN       | em0  | 10.0.2.15/24   | —                                      | Accès à internet     |
| LAN1      | em1  | 192.168.1.1/24 | 192.168.1.100/24 -<br>192.168.1.149/24 | Utilisateurs isolés  |
| LAN2      | em2  | 192.168.2.1/24 | 192.168.2.100/24 -<br>192.168.2.199/24 | Entreprise interne   |
| DMZ       | em3  | 10.10.10.1/24  | 10.10.10.10/24 -<br>10.10.10.30/24     | Héberge les serveurs |

### Adressage dans pfSense:

```

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***




WAN (wan)   -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)  -> em1 -> v4: 192.168.1.1/24
LAN2 (opt1) -> em2 -> v4: 192.168.2.1/24
DMZ (opt2)  -> em3 -> v4: 10.10.10.1/24


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

Enter an option:

```

### Organisation des ports dans l'interface Web de pfSense:

| Interface | Network port            |  |
|-----------|-------------------------|--|
| WAN       | em0 (08:00:27:05:d4:a9) |  |
| LAN1      | em1 (08:00:27:4a:9e:9d) |  Delete |
| LAN2      | em2 (08:00:27:48:49:76) |  Delete |
| DMZ       | em3 (08:00:27:80:98:d7) |  Delete |

 Save

### III. Répartition des services

DHCP :

Dans notre infrastructure réseau, le service DHCP est assuré par le routeur pfSense, qui attribue automatiquement des adresses IP aux machines des différents sous-réseaux.

Pour le LAN1, le DHCP distribue des adresses dans la plage 192.168.1.100 à 192.168.1.149, adaptée à un petit réseau réservé aux utilisateurs externes.

| Primary Address Pool |  |
|----------------------|--|
| Subnet               | 192.168.1.0/24   |
| Subnet Range         | 192.168.1.1 - 192.168.1.254  |
| Address Pool Range   | <div>192.168.1.100192.168.1.149</div> <div>FromTo</div> <div>The specified range for this pool must not be within the range configured on any other address pool for this interface.</div> |
| Additional Pools     | <div>+ Add Address Pool</div> <div>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</div>                            |

Pour le LAN2, la plage DHCP est 192.168.2.100 à 192.168.2.199, destinée à un réseau d'entreprise.

| Primary Address Pool |  |
|----------------------|--|
| Subnet               | 192.168.2.0/24   |
| Subnet Range         | 192.168.2.1 - 192.168.2.254  |
| Address Pool Range   | <div>192.168.2.100192.168.2.199</div> <div>FromTo</div> <div>The specified range for this pool must not be within the range configured on any other address pool for this interface.</div> |
| Additional Pools     | <div>+ Add Address Pool</div> <div>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</div>                            |

Enfin, dans la DMZ, le DHCP fournit des IP de 10.10.10.10 à 10.10.10.30, réservées aux serveurs accessibles depuis LAN2. Toutefois, les serveurs critiques peuvent également utiliser une IP statique.

The screenshot shows the 'Primary Address Pool' configuration page in pfSense. It includes fields for 'Subnet' (10.10.10.0/24) and 'Subnet Range' (10.10.10.1 - 10.10.10.254). The 'Address Pool Range' section has two input fields: 'From' (10.10.10.10) and 'To' (10.10.10.30). A note states: 'The specified range for this pool must not be within the range configured on any other address pool for this interface.' At the bottom, there is an 'Additional Pools' section with a '+ Add Address Pool' button and a note: 'If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.'

### Portail captif:

Le portail captif est mis en place uniquement sur le réseau LAN1, afin de contrôler l'accès au réseau des utilisateurs. Lorsqu'un client se connecte au LAN1, il est automatiquement redirigé vers une page d'authentification avant d'obtenir un accès à Internet. Ce mécanisme permet de filtrer les connexions, d'identifier les utilisateurs et de renforcer la sécurité du réseau. Le LAN2 et la DMZ ne sont pas concernés par ce portail captif, afin de préserver la fluidité de travail des machines techniques et des serveurs.



## Suivi des connexions dans l'interface Web de pfSense

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'Status / Captive Portal / lan1'. Below this, there's a section titled 'Users Logged In (1)'. It contains a table with the following data:

| IP address    | MAC address       | Username | Session start       | Actions |
|---------------|-------------------|----------|---------------------|---------|
| 192.168.1.100 | 08:00:27:30:24:5f | test     | 06/18/2025 16:27:39 |         |

Below the table, there are two buttons: 'Show Last Activity' and 'Disconnect All Users'.

### Pare-feu:

Le pare-feu est configuré sur toute l'infrastructure afin d'assurer un contrôle strict des communications entre les différentes zones du réseau.

Le LAN1, dédié aux utilisateurs externes, dispose seulement d'un accès à internet pour éviter tout risque de cyberattaque des hôtes qui constituent le LAN2.

The screenshot shows the 'Firewall / Rules / LAN1' configuration page in pfSense. The top navigation bar includes 'Firewall', 'Rules', and 'LAN1'. Below this, there's a section titled 'Rules (Drag to Change Order)'. It contains a table with the following data:

| States   | Protocol | Source       | Port | Destination  | Port   | Gateway | Queue | Schedule | Description              | Actions |
|--|----------|--------------|------|--------------|--------|---------|-------|----------|--------------------------|---------|
| <input checked="" type="checkbox"/> 1/1.32 MiB | *        | *            | *    | LAN1 Address | 443 80 | *       | *     |          | Anti-Lockout Rule        |         |
| <input type="checkbox"/> 0/0 B                 | IPv4 *   | LAN1 subnets | *    | LAN2 subnets | *      | *       | none  |          | Block access to LAN2     |         |
| <input type="checkbox"/> 0/0 B                 | IPv4 *   | LAN1 subnets | *    | DMZ subnets  | *      | *       | none  |          | Block access to DMZ      |         |
| <input type="checkbox"/> 7/219 KiB             | IPv4 *   | LAN1 subnets | *    | *            | *      | *       | none  |          | Allow access to internet |         |

Below the table, there are buttons: 'Add', 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and 'Separator'.

Le LAN2, destiné à l'entreprise, est autorisé à accéder à Internet ainsi qu'aux services disponibles dans la DMZ. Il est isolé du LAN1 afin de renforcer la sécurité.

Firewall / Rules / LAN2

Floating WAN LAN1 **LAN2** DMZ

Rules (Drag to Change Order)

|                          | States  | Protocol | Source       | Port | Destination  | Port | Gateway | Queue | Schedule | Description                | Actions |
|--------------------------|---------|----------|--------------|------|--------------|------|---------|-------|----------|----------------------------|---------|
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 *   | LAN2 subnets | *    | LAN1 subnets | *    | *       | none  |          |                            |         |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 *   | LAN2 subnets | *    | *            | *    | *       | none  |          | Allow access to everything |         |

Add Add Delete Toggle Copy Save Separator

La DMZ, qui héberge les serveurs, est strictement restreinte : elle ne peut initier aucune connexion vers les LAN, mais peut répondre aux requêtes provenant du LAN2.

Firewall / Rules / DMZ

Floating WAN LAN1 LAN2 **DMZ**

Rules (Drag to Change Order)

|                          | States  | Protocol | Source      | Port | Destination  | Port | Gateway | Queue | Schedule | Description              | Actions |
|--------------------------|---------|----------|-------------|------|--------------|------|---------|-------|----------|--------------------------|---------|
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 *   | DMZ subnets | *    | LAN2 subnets | *    | *       | none  |          | Block access to LAN2     |         |
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 *   | DMZ subnets | *    | LAN1 subnets | *    | *       | none  |          | Block access to LAN1     |         |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 *   | DMZ subnets | *    | *            | *    | *       | none  |          | Allow access to internet |         |

Add Add Delete Toggle Copy Save Separator

Cette politique de sécurité en zones renforce la protection globale du système tout en assurant le bon fonctionnement des services.

#### IV. Bonnes pratiques mises en place (sécurité et restrictions)

Un DHCP restreint :

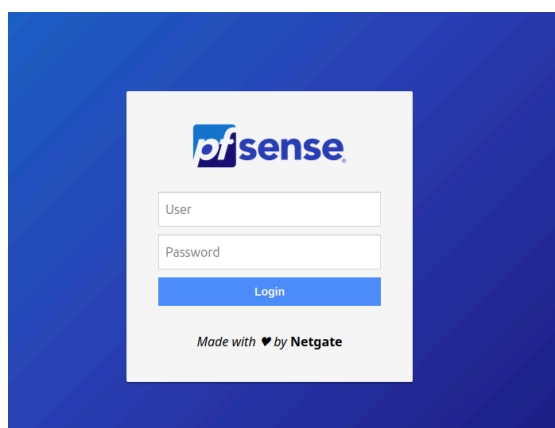
Chaque zone du réseau dispose d'un service DHCP configuré avec une plage d'adresses IP limitée, afin de réduire la surface d'attaque et de garder un meilleur contrôle sur les hôtes connectés. Seules les plages nécessaires sont allouées.

Règles de pare-feu :

Le pare-feu intégré à pfSense est configuré pour segmenter strictement les réseaux. Des règles sont définies pour autoriser uniquement le trafic nécessaire (ex : LAN2 → DMZ, LAN1 → Internet), et bloquer les accès non autorisés (ex : DMZ → LAN1/LAN2). Cette séparation permet de limiter les risques de compromission.

Connexion au portail captif :

Un portail captif est activé sur le réseau LAN1 pour obliger les utilisateurs à s'authentifier en locale via pfSense avant d'accéder au réseau. Cela permet de contrôler l'accès et d'identifier les utilisateurs, tout en empêchant les connexions non autorisées.



Sauvegarde quotidienne :

Un système de sauvegarde automatisée a été mis en place pour garantir la pérennité des données. Les sauvegardes de configuration sont

effectuées automatiquement tous les jours via le service intégré de pfSense. Cela permet de restaurer rapidement les configurations critiques en cas de panne ou de mauvaise manipulation.

Settings Restore Backup Now

### Auto Config Backup

**Enable ACB** ☒ Enable automatic configuration backups  
Auto Configuration Backup automatically encrypts configuration backup content using the Encryption Password below and then securely uploads the encrypted backup over HTTPS to Netgate servers.

**Backup Frequency**  
☐ Automatically backup on every configuration change  
☒ Automatically backup on a regular schedule

**Schedule**  
Minute (0-59) 0 Hours (0-23) 0 Day (1-31) 1 Month (1-12) \* Day of week (0-6) \*

## DNS sécurisé :

Le service DNS Resolver est activé sur le routeur pfSense. Il permet de résoudre les noms de domaine de manière récursive et sécurisée, tout en offrant la possibilité de gérer des noms internes. Ce service renforce la confidentialité des requêtes DNS et améliore la rapidité grâce à la mise en cache locale.

### General DNS Resolver Options

**Enable** ☒ Enable DNS resolver

**Listen Port** 53  
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

**Enable SSL/TLS Service** ☐ Respond to incoming SSL/TLS queries from local clients  
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

**SSL/TLS Certificate** GUI default (684bed2876043)  
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

**SSL/TLS Listen Port** 853  
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

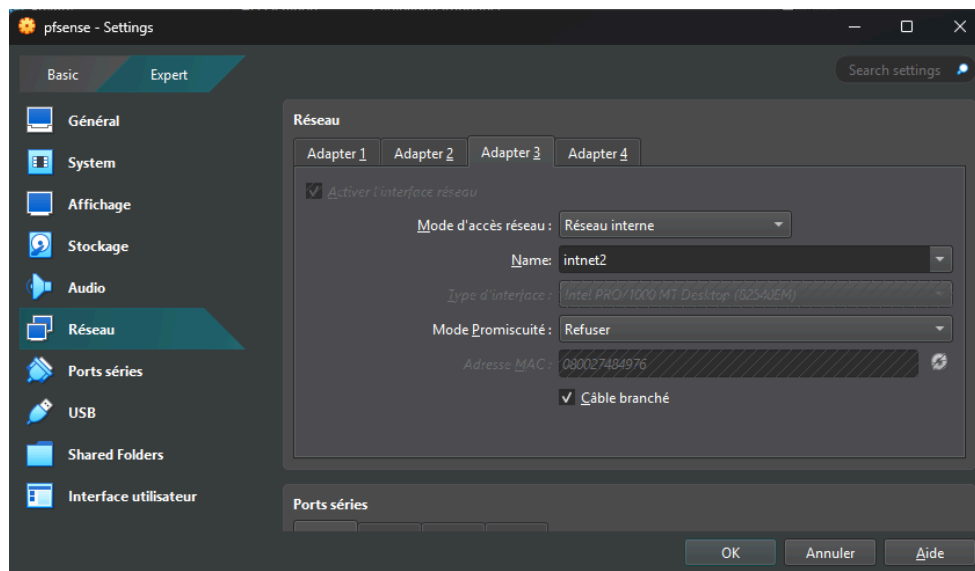
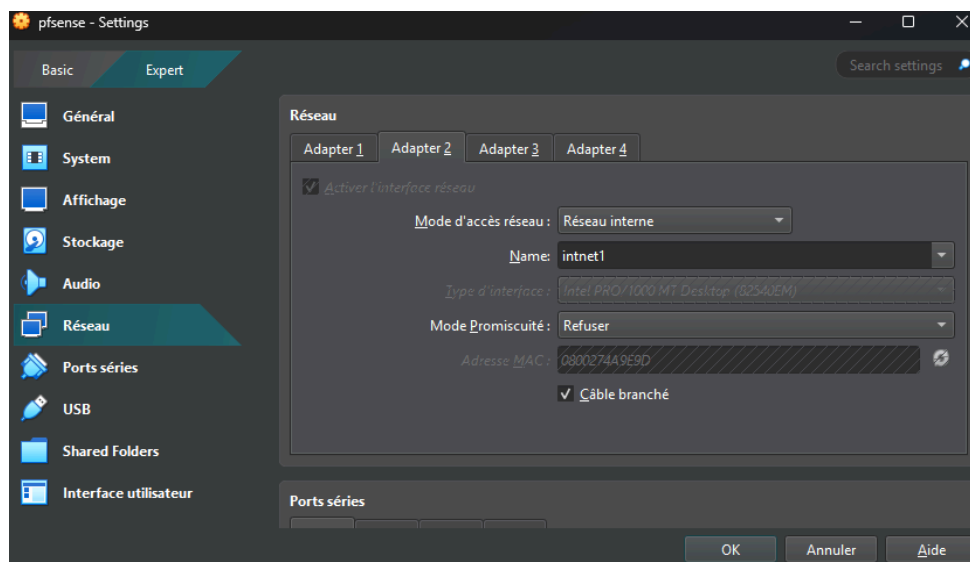
**Network Interfaces**  
All  
WAN  
LAN1  
LAN2  
DMZ  
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

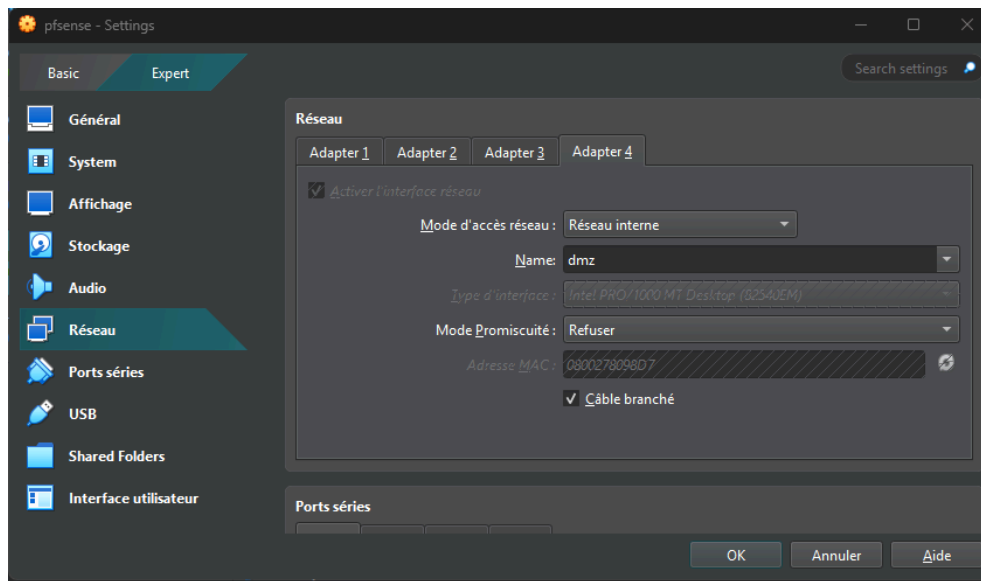
**Outgoing Network Interfaces**  
All  
WAN  
LAN1  
LAN2  
DMZ  
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

## V. Configuration des interfaces réseau dans Virtualbox



Dans VirtualBox, la maquette réseau a été construite en utilisant une combinaison de mode NAT et de réseaux internes pour isoler les différentes zones. L'interface WAN de la machine pfSense est configurée en mode NAT, permettant à l'ensemble du réseau d'accéder à Internet via la box de l'hôte. Les trois autres interfaces sont liées à des réseaux internes définis comme suit :



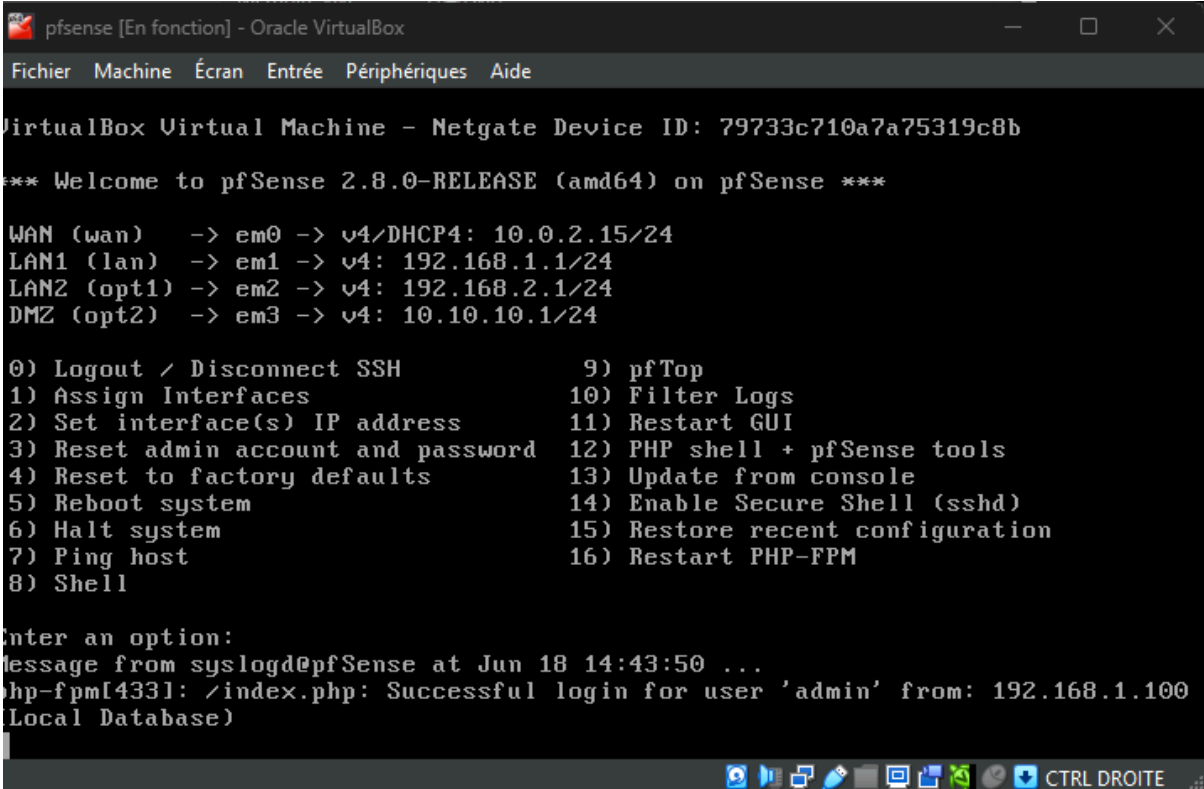


Ces réseaux internes permettent une séparation stricte des zones, sans communication directe avec l'extérieur sauf via le routeur.

## VI. Configuration des interfaces dans pfSense

Dans pfSense, après l'installation, les interfaces réseau ont été configurées manuellement en deux étapes :

- (1) Assign Interface – chaque interface physique (em0, em1, em2, em3) a été associée à une zone logique (WAN, LAN1, LAN2, DMZ)
- (2) Set Interface(s) IP address – chaque interface a ensuite reçu une adresse IP statique correspondant au plan d'adressage.



```
VirtualBox Virtual Machine - Netgate Device ID: 79733c710a7a75319c8b
*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

WAN (wan)    -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)   -> em1 -> v4: 192.168.1.1/24
LAN2 (opt1)  -> em2 -> v4: 192.168.2.1/24
DMZ (opt2)   -> em3 -> v4: 10.10.10.1/24

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

Enter an option:
Message from syslogd@pfSense at Jun 18 14:43:50 ...
php-fpm[4331]: /index.php: Successful login for user 'admin' from: 192.168.1.100
(Local Database)
```

Cette configuration permet à pfSense de jouer pleinement son rôle de routeur, pare-feu, serveur DHCP, DNS, et point de sortie vers Internet.