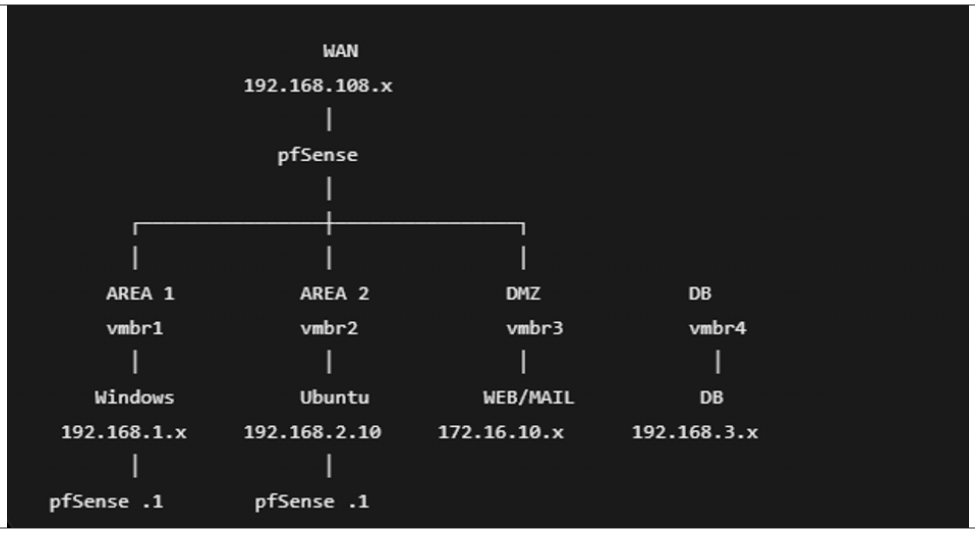
Infrastructure réseau segmentée avec DMZ

Pare-feu pfSense, zones cloisonnées et services Web / DNS / Mail sous Proxmox

1. Présentation et architecture

Cette infrastructure met en place un pare-feu pfSense virtualisé sous Proxmox, chargé de cloisonner quatre zones réseau distinctes : deux zones utilisateurs (AREA 1, AREA 2), une zone démilitarisée (DMZ) hébergeant les services exposés (Web, DNS, Mail), et une zone dédiée à la base de données. Chaque zone dispose de son propre bridge réseau virtuel et de sa propre interface sur pfSense, ce qui permet de définir des règles de filtrage indépendantes entre zones.



- WAN : 192.168.108.x — connexion au réseau physique existant
- AREA 1 (vmbr1) : 192.168.1.x — poste Admin interne Windows
- AREA 2 (vmbr2) : 192.168.2.x — poste Admin interne Ubuntu
- DMZ (vmbr3) : 172.16.10.x — serveurs Web, DNS et Mail
- DB (vmbr4) : 192.168.3.x — serveur de base de données Windows

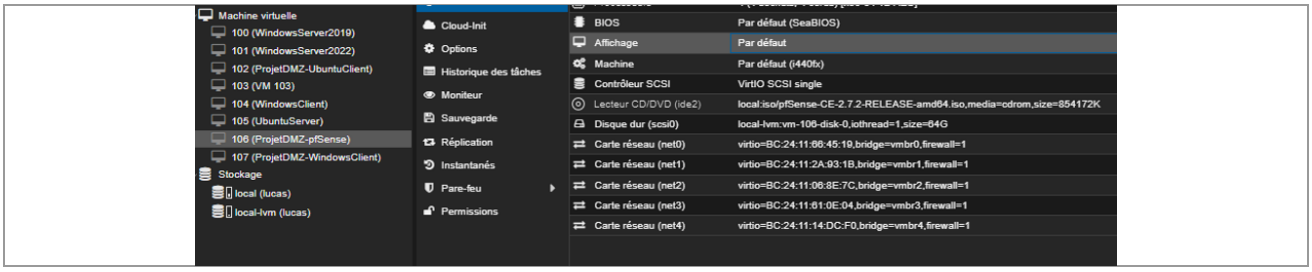
2. Segmentation réseau sur Proxmox

Quatre bridges Linux supplémentaires sont créés sur l'hôte Proxmox, en plus du bridge par défaut vmbr0 relié au réseau physique. Chacun matérialise une zone de l'infrastructure et ne relie entre elles que les VM qui y sont explicitement rattachées, sans carte physique associée : l'étanchéité entre zones dépend donc uniquement des règles appliquées sur pfSense, seul point de passage entre les bridges.

vmbr1	Linux Bridge	Non	Oui	Non	AREA1
vmbr2	Linux Bridge	Non	Oui	Non	AREA 2
vmbr3	Linux Bridge	Non	Oui	Non	DMZ, WEB/DNS + MAIL
vmbr4	Linux Bridge	Non	Oui	Non	serveur DB

3. Machine virtuelle pfSense

La VM pfSense reçoit cinq cartes réseau virtuelles, chacune reliée à un bridge différent : la première (net0) vers vmbr0 pour l'accès WAN, puis une carte par zone interne (net1 à net4) vers vmbr1, vmbr2, vmbr3 et vmbr4. C'est cette VM qui assurera tout le routage et le filtrage entre les zones :



4. Installation et attribution des interfaces pfSense

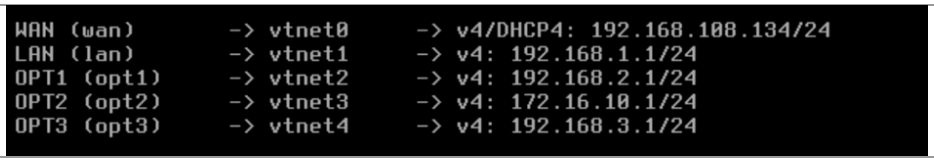
Lors de l'installation, pfSense détecte les cinq interfaces virtuelles (vtnet0 à vtnet4) et demande leur rôle logique. L'ordre suit celui des cartes réseau définies dans Proxmox :



- WAN → vtnet0 (vmbr0, réseau physique existant)
- LAN → vtnet1 (vmbr1, AREA 1)
- OPT1 → vtnet2 (vmbr2, AREA 2)
- OPT2 → vtnet3 (vmbr3, DMZ)
- OPT3 → vtnet4 (vmbr4, DB)

4.1 Adressage IP des interfaces

Chaque interface reçoit ensuite une adresse IP fixe côté pfSense, qui fera office de passerelle pour la zone correspondante. Seule l'interface WAN reste en DHCP, héritant d'une adresse du réseau physique existant :

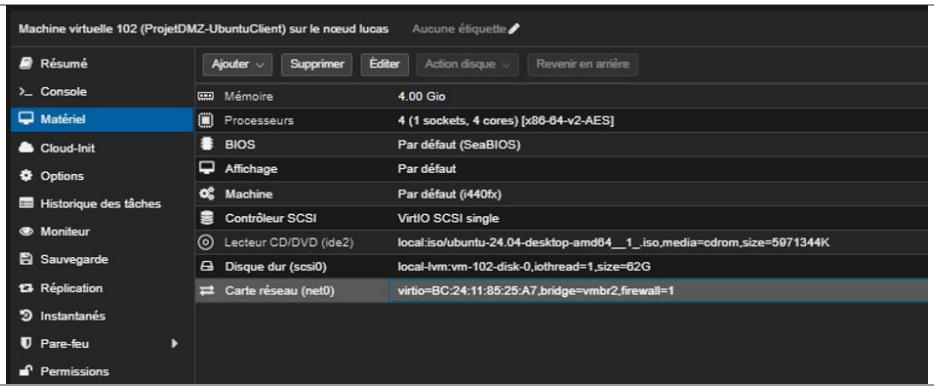


- WAN : DHCP → 192.168.108.134/24
- LAN (AREA 1) : 192.168.1.1/24
- OPT1 (AREA 2) : 192.168.2.1/24
- OPT2 (DMZ) : 172.16.10.1/24
- OPT3 (DB) : 192.168.3.1/24

5. Déploiement des postes et serveurs par zone

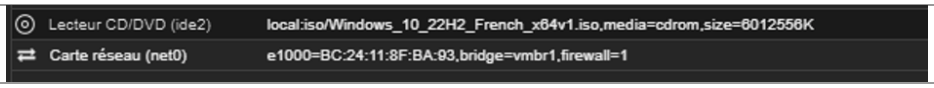
5.1 Admin interne Poste Ubuntu — AREA 2

Une VM Ubuntu Desktop est rattachée au bridge vmbr2, la plaçant directement dans la zone AREA 2, derrière l'interface OPT1 de pfSense :

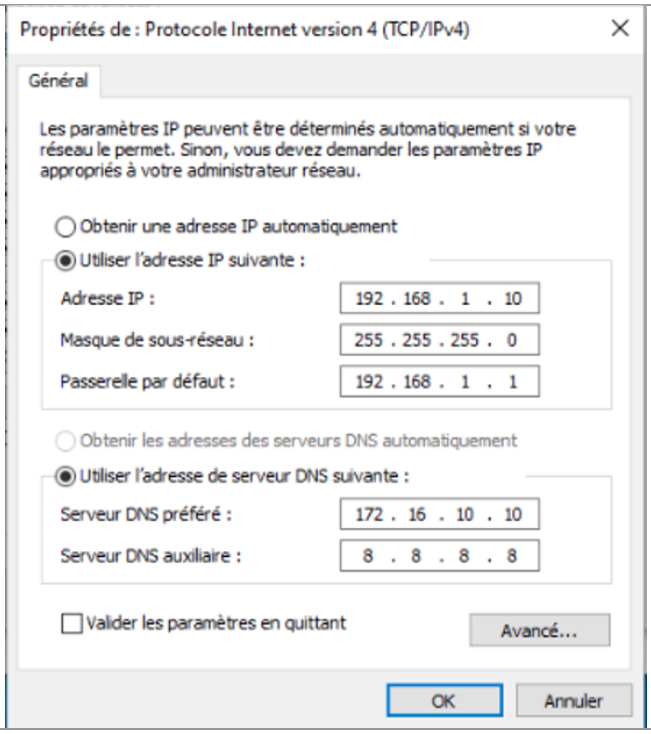


5.2 Admin interne Poste Windows — AREA 1

Le poste Admin interne Windows est raccordé au bridge vmbr1 (AREA 1) :

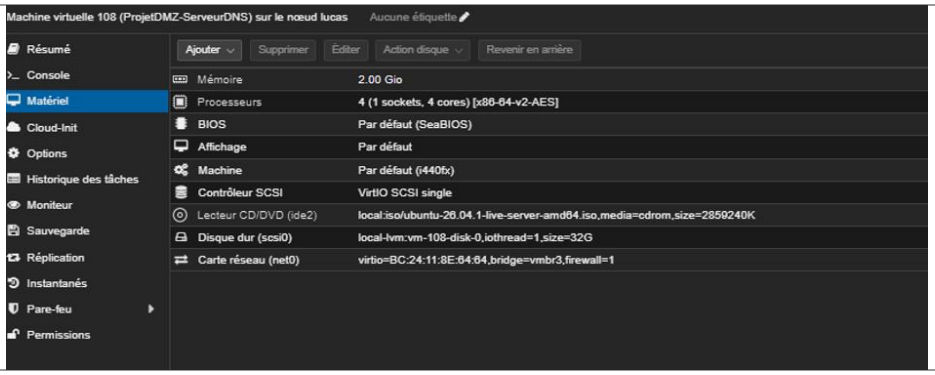


Son adressage IP est configuré manuellement, avec pfSense (192.168.1.1) comme passerelle et le futur serveur DNS de la DMZ (172.16.10.10) déclaré comme résolveur principal :

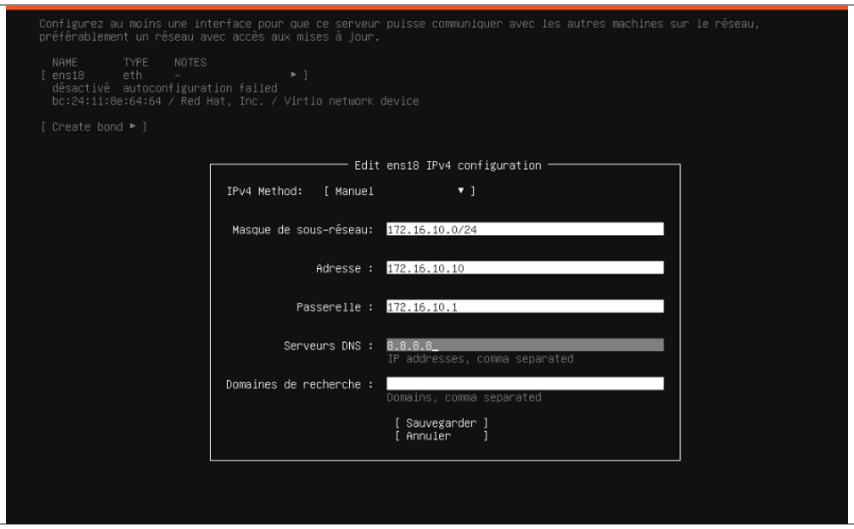


5.3 Serveur DNS / Web — DMZ

Un serveur Ubuntu Server est déployé dans la DMZ, rattaché au bridge vmbr3. Il hébergera à la fois le service DNS (BIND) et le service Web (Apache) de la zone :



Lors de l'installation, l'interface réseau est configurée manuellement avec l'adresse 172.16.10.10/24, la passerelle pfSense de la DMZ (172.16.10.1) et un DNS public temporaire :

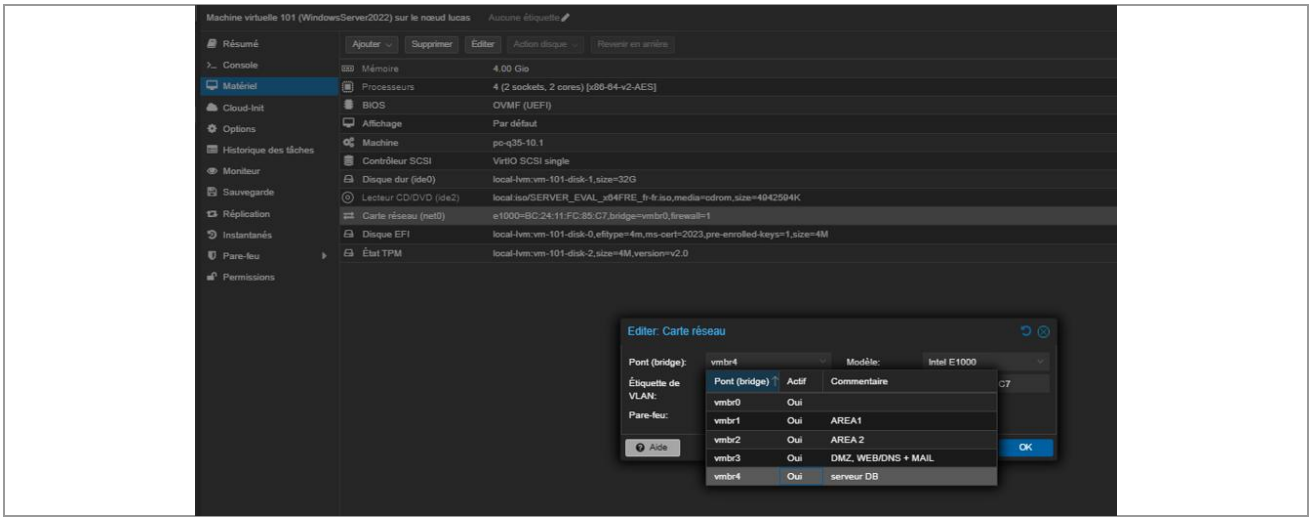


Le compte système du serveur est créé sous l'identifiant serveurdns :

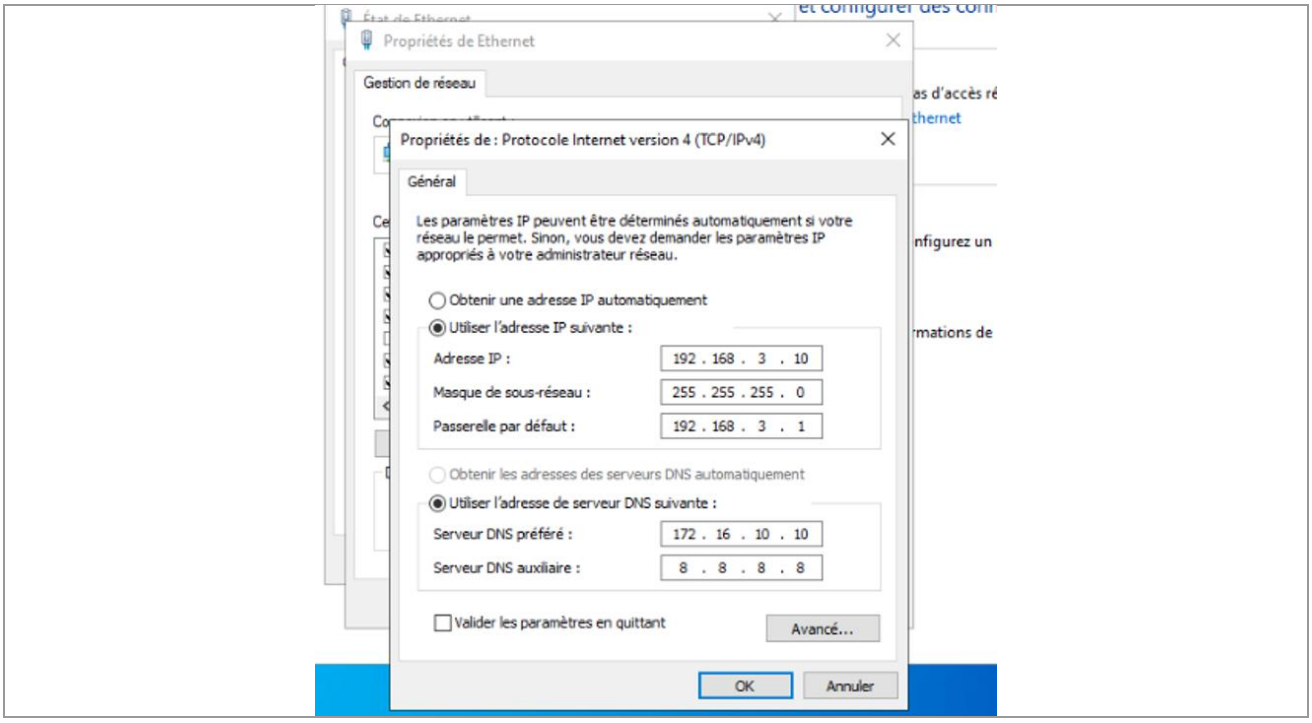


5.4 Serveur DB — Windows Server

Le serveur de base de données est une VM Windows Server dont la carte réseau est rattachée au bridge vmbr4, correspondant à la zone DB isolée derrière l'interface OPT3 de pfSense :



Son adressage IP final place le serveur dans le réseau 192.168.3.0/24, avec pfSense comme passerelle et le serveur DNS de la DMZ comme résolveur :



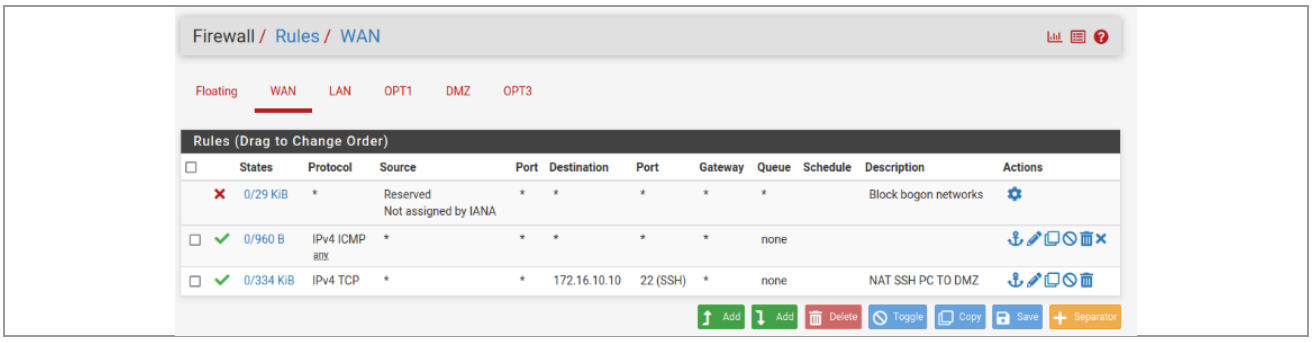
- Adresse IP : 192.168.3.10 / 255.255.255.0
- Passerelle : 192.168.3.1
- DNS préféré : 172.16.10.10 — DNS auxiliaire : 8.8.8.8

6. Règles de pare-feu pfSense

Par défaut, pfSense bloque tout trafic entrant sur chaque interface : c'est l'ensemble des règles définies onglet par onglet (WAN, LAN, OPT1, DMZ, OPT3) qui autorise explicitement les flux nécessaires au fonctionnement de l'infrastructure, zone par zone.

6.1 Configuration WAN

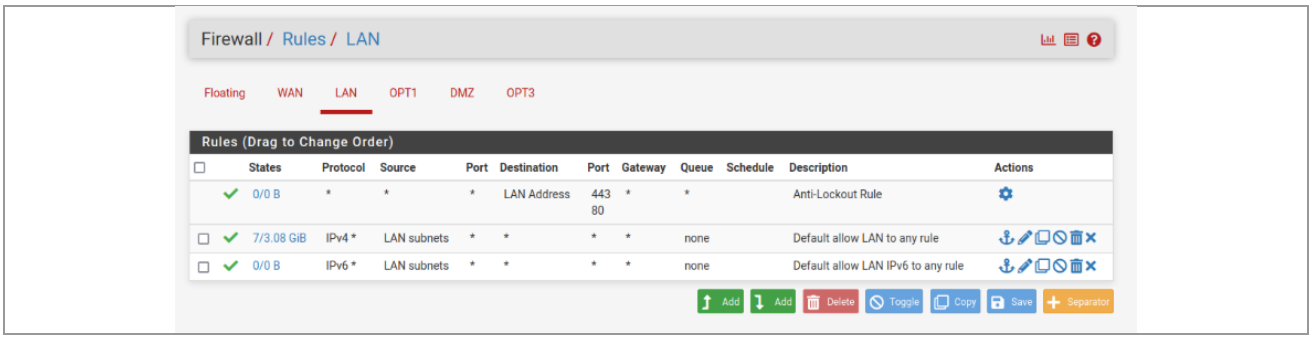
Sur l'interface WAN, le trafic entrant depuis l'extérieur est strictement limité. Une règle bloque par défaut les réseaux bogon (adresses non attribuées par l'IANA), l'ICMP est autorisé pour permettre les tests de ping, et une règle de NAT redirige les connexions SSH entrantes vers le serveur de la DMZ :



- Block bogon networks — blocage des réseaux non attribués (règle par défaut pfSense)
- IPv4 ICMP any — autorisation du ping entrant depuis le WAN
- NAT SSH PC to DMZ — redirection du port 22 entrant vers 172.16.10.10 (serveur DMZ)

6.2 Configuration LAN

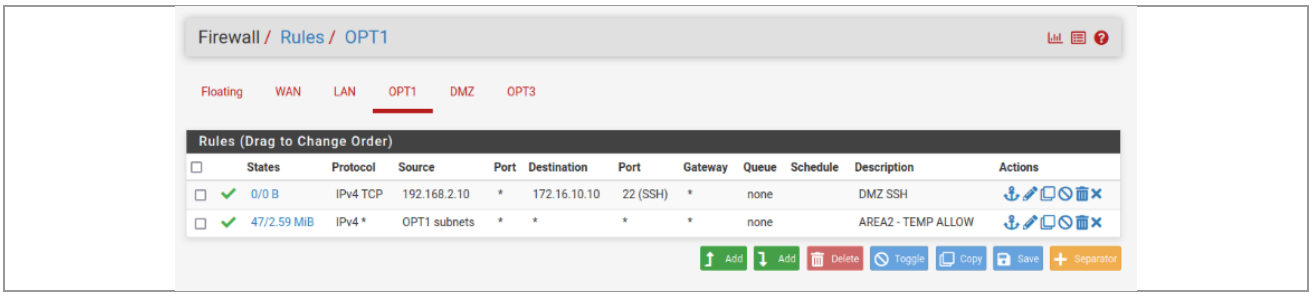
L'interface LAN (réseau d'administration de pfSense) conserve les règles par défaut : la règle anti-lockout protège l'accès à l'interface web de pfSense, et le trafic LAN vers n'importe quelle destination est autorisé sans restriction, en IPv4 comme en IPv6 :



- Anti-Lockout Rule — accès garanti à l'interface d'administration pfSense (ports 80/443)
- Default allow LAN to any rule — sortie libre pour le réseau d'administration
- Default allow LAN IPv6 to any rule — équivalent en IPv6

6.3 Configuration OPT1 (AREA 2)

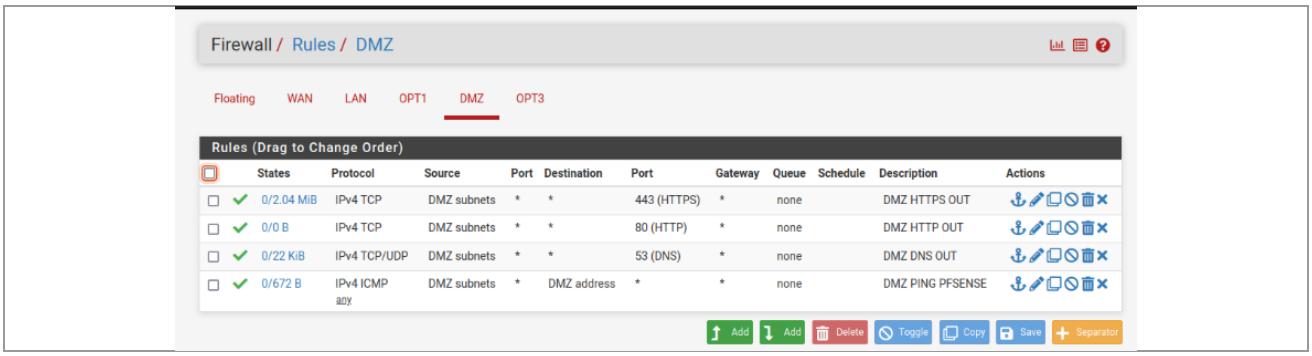
La zone AREA 2 dispose d'une règle ciblée autorisant uniquement le poste Admin interne Ubuntu (192.168.2.10) à joindre le serveur DMZ en SSH, ainsi qu'une règle temporaire plus permissive utilisée pendant la phase de mise en place et de tests :



- DMZ SSH — 192.168.2.10 autorisé en TCP vers 172.16.10.10, port 22 uniquement
- AREA2 - TEMP ALLOW — autorisation large temporaire de tout le sous-réseau OPT1, à resserrer une fois les tests validés

6.4 Configuration DMZ

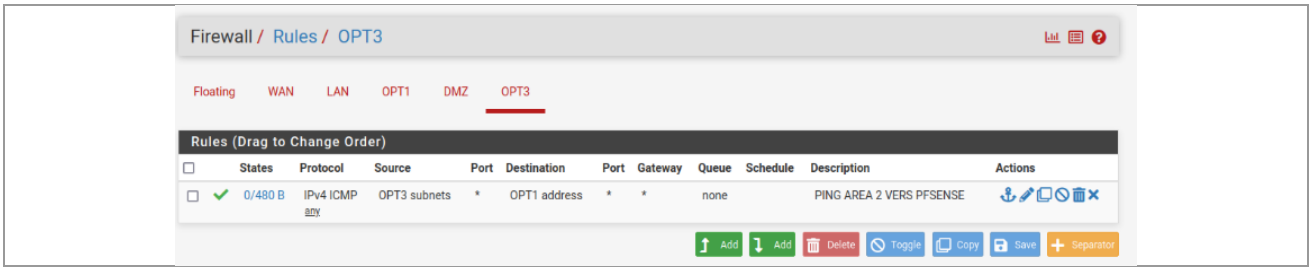
Les serveurs de la DMZ ne sont autorisés à initier du trafic sortant que sur les ports strictement nécessaires à leur fonctionnement : HTTPS et HTTP pour les mises à jour et le service Web, DNS pour les résolutions, et ICMP pour pouvoir pinguer pfSense lui-même à des fins de diagnostic :



- DMZ HTTPS OUT — sortie TCP/443 pour les sous-réseaux DMZ
- DMZ HTTP OUT — sortie TCP/80 pour les sous-réseaux DMZ
- DMZ DNS OUT — sortie TCP/UDP 53 pour les sous-réseaux DMZ
- DMZ PING PFSENSE — ICMP autorisé des sous-réseaux DMZ vers l'adresse de pfSense

6.5 Configuration OPT3 (DB)

La zone DB, la plus sensible, ne dispose que d'une règle minimale autorisant le ping vers l'interface OPT1 de pfSense (AREA 2), utilisée pour valider la connectivité inter-zones sans ouvrir de flux applicatif :



- PING AREA 2 VERS PFSENSE — ICMP autorisé des sous-réseaux OPT3 vers l'adresse OPT1

Cette politique par défaut « tout bloqué sauf explicitement autorisé » explique directement les résultats des tests de connectivité réalisés plus loin dans ce document : la DMZ répond car elle dispose de règles de sortie et le NAT WAN cible son adresse, tandis qu'AREA 2 reste injoignable depuis l'extérieur en l'absence de toute règle WAN pointant vers 192.168.2.0/24.

7. Vérification réseau côté Linux

Sur les machines Linux (client AREA 2, serveurs de la DMZ), trois commandes suffisent à vérifier rapidement l'adressage IP, la route par défaut et la résolution DNS en cours :

```
ip addr show
ip route
resolvectl status
```

Une fois le serveur DNS de la DMZ opérationnel, l'Admin interne Ubuntu de la zone AREA 2 doit afficher ce serveur (172.16.10.10) comme résolveur DNS courant :



8. Configuration du serveur Web / DNS (172.16.10.10)

Les paquets nécessaires sont installés : Apache pour le service Web, BIND9 pour le DNS, ainsi qu'un serveur SSH pour l'administration à distance :

```
sudo apt update
sudo apt install apache2 bind9 bind9-utils dnsutils -y
sudo apt install openssh-server -y

systemctl status apache2
curl http://172.16.10.10
```

La page par défaut d'Apache confirme que le service Web répond correctement sur son adresse.

8.1 Déclaration de la zone DNS

La zone dmz.test est déclarée dans la configuration locale de BIND, puis son fichier de zone est créé avec les enregistrements du domaine :

```
sudo nano /etc/bind/named.conf.local

zone "dmz.test" {
    type master;
    file "/etc/bind/db.dmz.test";
};
```

Pour enregistrer et quitter nano : Ctrl+O puis Entrée pour enregistrer, puis Ctrl+X pour quitter.

```
sudo nano /etc/bind/db.dmz.test

$TTL 86400

@   IN  SOA dns.dmz.test. admin.dmz.test. (
        2026093001
        3600
        1800
        604800
        86400
)

@       IN  NS  dns.dmz.test.
@       IN  A   172.16.10.10
dns     IN  A   172.16.10.10
web     IN  A   172.16.10.10
```

Pour enregistrer et quitter nano : Ctrl+O puis Entrée pour enregistrer, puis Ctrl+X pour quitter.

La configuration et la zone sont validées avant de redémarrer le service, puis un test de résolution locale confirme le bon fonctionnement :

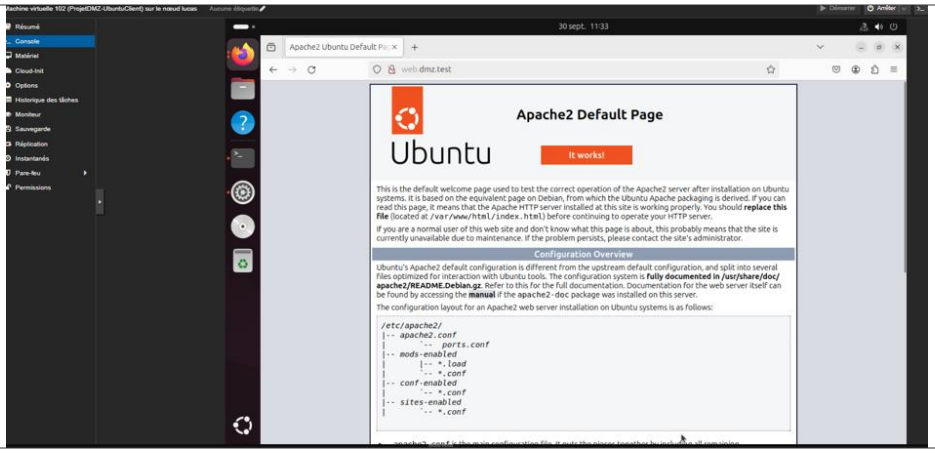
```
sudo named-checkconf
sudo named-checkzone dmz.test /etc/bind/db.dmz.test
sudo systemctl restart named
dig @127.0.0.1 web.dmz.test
```

9. Test depuis AREA 2 vers la DMZ

Depuis l'Admin interne Ubuntu de la zone AREA 2, la résolution DNS et l'accès Web vers la DMZ sont testés successivement en ligne de commande, puis validés depuis le navigateur avec le nom de domaine complet :

```
dig @172.16.10.10 web.dmz.test
curl http://172.16.10.10
curl http://web.dmz.test
```

Le navigateur du client AREA 2 affiche bien la page par défaut d'Apache en interrogeant directement le nom web.dmz.test, preuve que le routage inter-zones et la résolution DNS fonctionnent de bout en bout :



9.1 DNS permanent sur AREA 2

Le serveur DNS de la DMZ est fixé de façon persistante sur la connexion réseau de l'Admin interne Ubuntu, afin qu'il ne soit pas écrasé par une éventuelle configuration DHCP :

```
nmcli connection show
# Connexion identifiée : netplan-ens18

sudo nmcli connection modify netplan-ens18 ipv4.dns "172.16.10.10"
sudo nmcli connection modify netplan-ens18 ipv4.ignore-auto-dns yes
sudo nmcli connection up netplan-ens18

dig web.dmz.test
```

10. Serveur Mail (172.16.10.20)

Un second serveur est déployé dans la DMZ pour héberger le service de messagerie : Postfix pour le transport SMTP, Dovecot pour l'accès IMAP/POP3 :

```
sudo apt update
sudo apt install postfix dovecot-imapd dovecot-pop3d mailutils openssh-server -y
```

Lors de l'installation de Postfix, les valeurs suivantes sont renseignées :

- Type de configuration : Internet Site
- System mail name : dmz.test

Les deux services sont ensuite vérifiés :

```
systemctl status postfix
systemctl status dovecot
```

10.1 Adressage IP statique du serveur Mail

L'adresse IP du serveur Mail est fixée directement dans sa configuration Netplan, avec pour passerelle et résolveur les mêmes adresses que le reste de la DMZ :

```
sudo nano /etc/netplan/50-cloud-init.yaml

network:
  version: 2
  ethernets:
    ens18:
      dhcp4: false
      addresses:
        - 172.16.10.20/24
      routes:
        - to: default
          via: 172.16.10.1
      nameservers:
        addresses:
          - 172.16.10.10
```

Pour enregistrer et quitter nano : Ctrl+O puis Entrée pour enregistrer, puis Ctrl+X pour quitter.

La configuration est validée puis appliquée, avant de tester la passerelle et la résolution DNS :

```
sudo netplan generate
sudo netplan apply

ping -c 3 172.16.10.1
dig @172.16.10.10 web.dmz.test
```

11. Windows Server DB — récapitulatif

La configuration finale du serveur de base de données est vérifiée avec ipconfig, puis la passerelle pfSense de sa zone est testée :

- IP : 192.168.3.10 / 255.255.255.0
- Passerelle : 192.168.3.1
- DNS : 172.16.10.10

12. Routage et vérification depuis le poste WAN externe

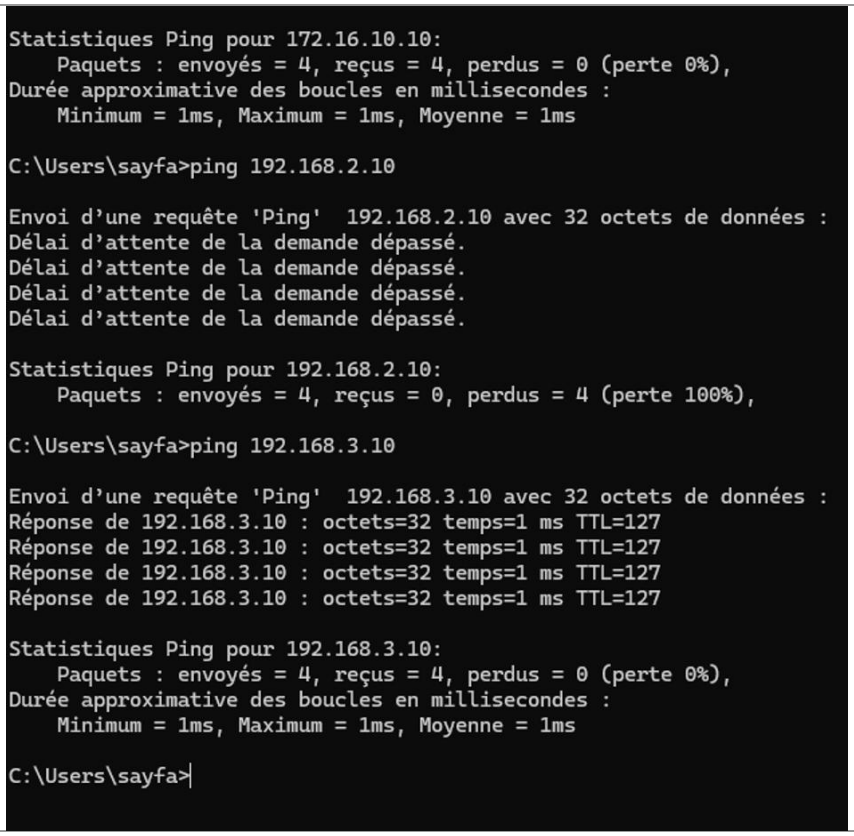
Depuis un poste situé sur le réseau externe (WAN, hors des zones internes), des routes statiques sont ajoutées afin de pouvoir joindre la DMZ et le réseau DB à travers pfSense, qui fait office de passerelle :

```
route -p add 172.16.10.0 mask 255.255.255.0 192.168.108.134
route -p add 192.168.3.0 mask 255.255.255.0 192.168.108.134
route print
```

Trois cibles sont ensuite testées depuis ce poste externe : le serveur Web/DNS de la DMZ, le serveur Mail de la DMZ et le serveur DB :

```
ping 172.16.10.10
ping 172.16.10.20
ping 192.168.3.10
```

Les résultats confirment le comportement attendu du pare-feu : la DMZ (172.16.10.10) et le réseau DB (192.168.3.10) répondent normalement depuis l'extérieur, tandis qu'une tentative de ping vers l'AREA 2 (192.168.2.10) échoue systématiquement — cette zone utilisateur n'est, à raison, pas exposée depuis le WAN :



13. Conclusion

Cette maquette illustre une architecture réseau segmentée classique en entreprise : un pare-feu central (pfSense) arbitre les échanges entre zones utilisateurs, zone démilitarisée et zone de données, chacune isolée sur son propre bridge Proxmox. Les tests réalisés depuis le réseau externe confirment le comportement attendu d'une DMZ bien configurée : les services volontairement exposés (Web, DNS, futur Mail) et le serveur de données restent joignables, tandis que les postes utilisateurs internes (AREA 1, AREA 2) restent invisibles depuis l'extérieur. Cette base est directement extensible avec des règles de filtrage plus fines par port et par protocole sur chaque interface de pfSense.

Infrastructure montée dans un cadre pédagogique, sur un réseau de laboratoire isolé. Les routes statiques ajoutées côté client (route -p add) et les règles de pare-feu associées ne doivent être reproduites que sur des réseaux dont on est propriétaire ou pour lesquels une autorisation explicite a été obtenue.