



Rapport

4ème année
Ingénieur Informatique & Réseaux

*Création d'une DMZ
virtuelle (Web + DB + FW)
dans Proxmox*

Réalisé par : IMANE Chakrellah
YASSINE Ech-chaoui

Prof: Pr.Ouadou

2024-2025

Table des matières

Introduction Générale	3
Outils nécessaires.....	4
1. Installation de Proxmox.....	4
2. Configuration réseau dans Proxmox	4
3. Création des machines virtuelles	5
Préparation :.....	5
pfSense (Firewall)	6
1.Objectif du projet :	9
2. Architecture du système	9
3. Préparation de l'environnement de travail dans VMware.....	9
4. Création et configuration des machines virtuelles.....	10
4.1. Création de la VM pfSense	10
Configuration IP de base	11
4.2. Création des deux serveurs Web.....	11
Serveur Web 1 (connecté au LAN)	11
Serveur Web 2 (connecté à la DMZ).....	12
Instalation des Roles IIS sur les deux Serveur :	12
5. Configuration des composants.....	13
5.1 Accès à l'interface web :.....	13
5.2. Présentation de l'Interface	13
5.3. Règles de Pare-feu.....	14
Conclusion Générale.....	24

Introduction Générale

Ce projet de **création d'une DMZ virtuelle sous Proxmox** vise à implémenter une architecture réseau sécurisée, simulant un environnement de production réel avec des services critiques exposés de manière contrôlée. L'objectif principal est de :

1. **Segmenter le réseau** en zones de sécurité distinctes (WAN, LAN, DMZ) pour isoler les services exposés (comme un serveur web) des infrastructures sensibles (comme une base de données).
2. **Configurer pfSense** comme firewall/pare-feu pour filtrer le trafic, gérer les règles NAT (Port Forwarding), et assurer une protection contre les accès non autorisés.
3. **Déployer des serveurs virtuels** (Web + SQL) dans des environnements cloisonnés, reflétant les bonnes pratiques en matière de sécurité réseau.
4. **Valider la connectivité** en testant l'accès aux services tout en garantissant que les flux respectent les politiques de sécurité définies.

Ce projet aborde ainsi des compétences clés en **virtualisation, routage, pare-feu, et administration système**, tout en illustrant l'importance d'une architecture défensive dans les infrastructures modernes.

Outils nécessaires

- **Proxmox VE** (dernière version)
- **ISO pfSense** (dernière version CE)
- **Windows Server 2022** (ISO)
- **Navigateur web** (pour accéder à l'interface Proxmox et pfSense)

1. Installation de Proxmox

1. Télécharger l'ISO de Proxmox VE
2. Installer sur un serveur physique ou virtualisé
3. Configurer le réseau (IP statique)

2. Configuration réseau dans Proxmox

Créer les bridges réseau nécessaires :

The screenshot shows the Proxmox VE interface with the 'Network' list. The 'Create' button in the top right is highlighted with a red box. The 'Network' item in the left sidebar is also highlighted with a red box.

Name	Type	Active	Autostart	VLAN a...	Ports/Staves	Bond Mode	CIDR	Gateway	Com...
ens33	Network Device	Yes	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	ens33		192.168.198.10/24	192.168.100.1	

1. Cliquez sur "Create" > "Linux Bridge"
2. Ajoutez **vmbr1** (LAN) avec ces paramètres :
 - **Name** : vmbr1
 - **Bridge ports** : *laisser vide*
 - **Autostart** :
 - *Ne pas mettre d'adresse IP*
3. Répétez pour **vmbr2** (DMZ) :
 - **Name** : vmbr2
 - Tous les autres champs vides sauf Autostart
4. Ne touchez pas à **vmbr0** (risque de déconnexion)

The dialog box for creating a Linux Bridge has the following fields:

- Name: vmbr1
- Autostart:
- VLAN aware:
- Bridge ports: (empty)
- IPv4/CIDR: (empty)
- Gateway (IPv4): (empty)
- IPv6/CIDR: (empty)
- Gateway (IPv6): (empty)
- Comment: (empty)

Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
vmbr0	Linux Bridge	Yes	Yes		ens33		192.168.198.10/24	192.168.100.1	
vmbr1	Linux Bridge	No	Yes						
vmbr2	Linux Bridge	No	Yes						

Pending changes (Either reboot or use 'Apply Configuration' (needs ifupdown2) to activate)

```
... /etc/network/interfaces 2025-04-15 09:58:20.890805588 +0100
... /etc/network/interfaces.new 2025-05-11 00:23:32.009096316 +0100
#> 1: ens33
#> network interface settings; autogenerated
#> Please do NOT modify this file directly, unless you know what
#> you're doing.
#>
#> If you want to manage parts of the network configuration manually,
```

3. Création des machines virtuelles

Préparation :

- Téléchargez l'ISO pfSense : <https://www.pfsense.org/download/>
- Upload dans Proxmox : Datacenter > storage > local (pve) > Content > Upload

Name	Date	Format	Size
SERVER_EVAL_x64FRE_en-us.iso	2025-05-11 19:05:42	iso	5.04 GB
pfsense-CE-2.7.2-RELEASE-amd64.iso	2025-05-11 18:52:07	iso	87.67 MB
ubuntu-22.04.5-live-server-amd64.iso	2025-05-11 19:28:42	iso	2.14 GB

pfSense (Firewall)

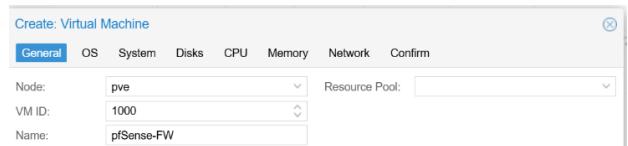
1.

2. Création de la VM :

Clic droit sur le nœud > Create VM

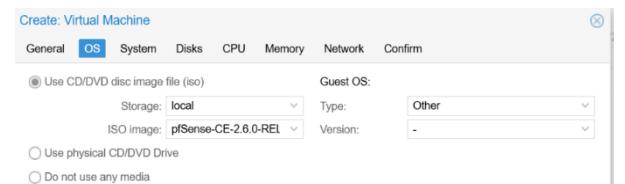
o General :

- Nom : pfSense-FW
- ID VM : 100 (recommandé pour le firewall)



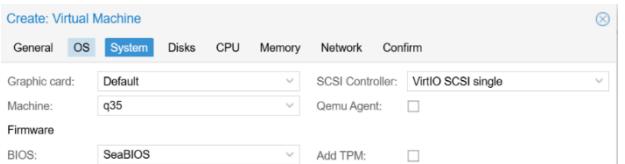
o OS :

- ISO : sélectionnez pfSense
-
- Type : BSD (other)



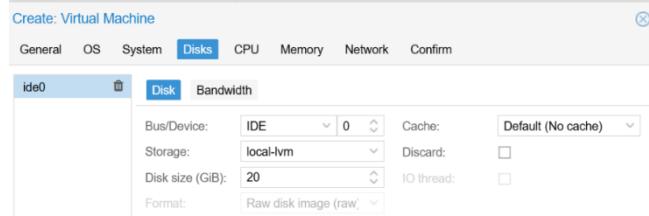
o System :

- Graphic : Default
- Machine : q35
- BIOS : SeaBIOS



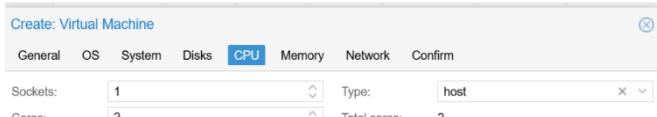
o Disks :

- Taille : 20GB (thin allocation)
- Storage : local-lvm



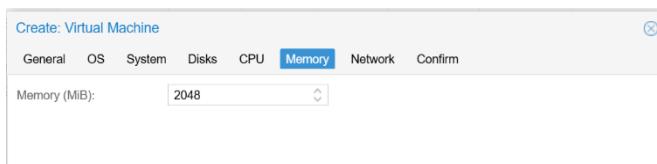
o CPU :

- Cores : 2
- Type : host



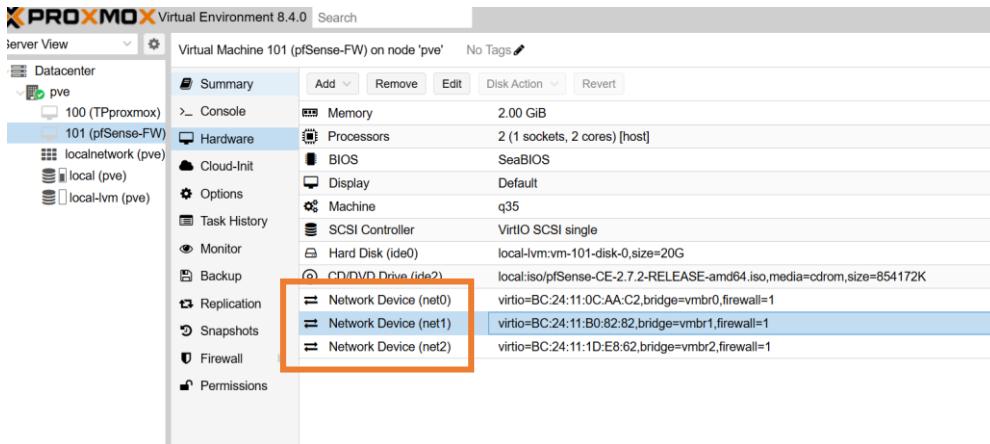
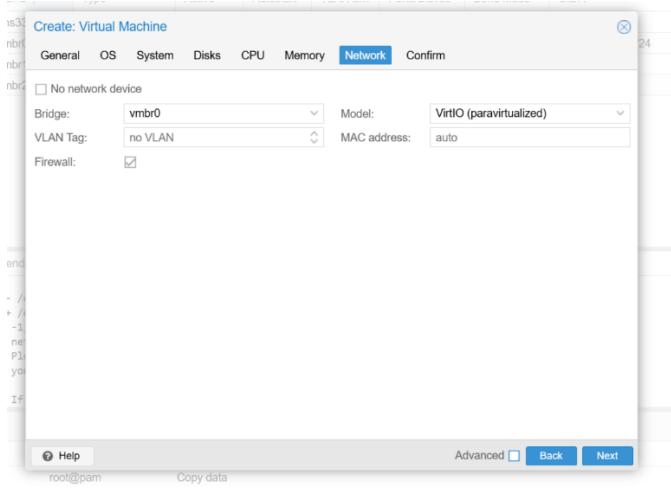
o Memory :

- 2048 MB (fixe, sans ballooning)



- **Network :**

- Interface 0 : vmbr0 (WAN) - modèle virtio
- Interface 1 : vmbr1 (LAN) - modèle virtio
- Interface 2 : vmbr2 (DMZ) - modèle virtio



1. **Démarrer et configurer pfSense :**

- Console > Start > Console
- Installation :
 - Acceptez les options par défaut
 - Partitionnement : Auto (UFS)
- Configuration réseau :
 - Assigner interfaces :
 - vtnet0 = WAN
 - vtnet1 = LAN
 - vtnet2 = DMZ
 - IP LAN : 192.168.1.1/24
 - IP DMZ : 192.168.2.1/24

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.198.135/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.2.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator 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: █
```

Contraintes de Stockage avec Proxmox et Justification du Changement d'Hyperviseur

Lors de la mise en place de l'environnement de virtualisation avec **Proxmox VE**, nous avons rencontré une contrainte technique majeure liée à la **capacité de stockage**. En effet, l'utilisation de plusieurs machines virtuelles (pfSense, serveur Web, serveur Base de Données) ainsi que le besoin de stocker plusieurs images ISO (systèmes d'exploitation, outils) nécessitent un **espace disque important**. Nous avons exploré plusieurs solutions pour contourner ce problème :

1. **Utilisation de WinSCP** pour transférer les fichiers ISO, mais cela a été entravé par un problème de permission lié à une autre configuration du système.
2. **Ajout d'un nouveau stockage local dans Proxmox (local-lvm)**, mais cela s'est révélé inefficace car cela créait une copie parallèle du stockage existant, sans réelle extension.
3. **Recréation de la VM Proxmox dans VMware avec un disque plus grand**, mais cela ajoutait encore plus de complexité et de consommation d'espace.

Face à ces limitations, mon binôme et moi avons pris la décision de **basculer vers un hyperviseur de type 2, VMware Workstation**, qui nous offrait une **gestion plus souple du stockage** et une configuration plus stable dans notre environnement local. Il est important de souligner que **la méthode de travail, l'architecture du projet, et la configuration réseau restent identiques**, seul l'hyperviseur a été remplacé. Cette adaptation nous a permis de continuer le projet dans de meilleures conditions techniques, tout en respectant les objectifs pédagogiques initiaux.

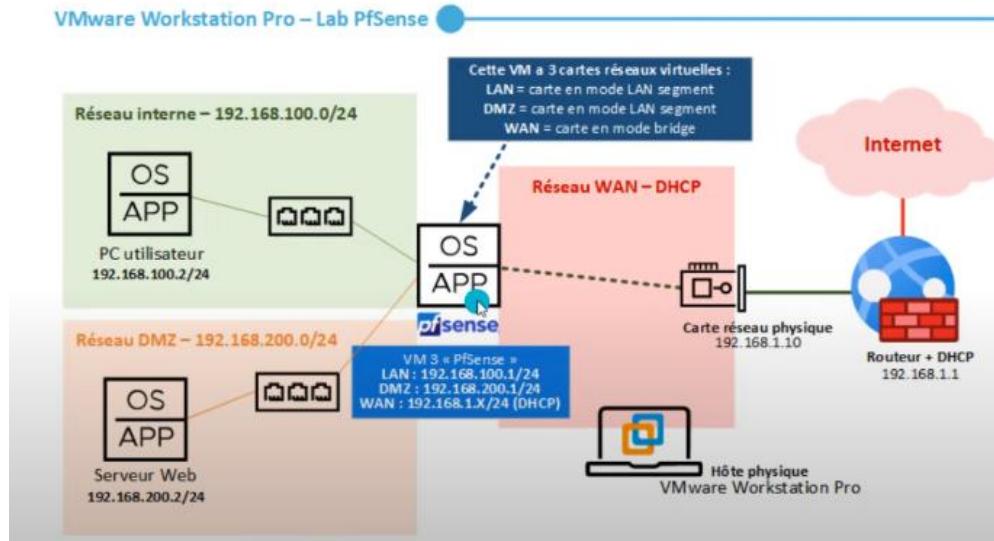
1. Objectif du projet :

Créer un environnement réseau sécurisé avec :

- Un firewall (pfSense) gérant 3 zones (LAN, DMZ, WAN).
- Deux serveurs web (Windows Server 2022) dans des zones distinctes (LAN + DMZ).
- **Outils utilisés** : VMware Workstation Pro, pfSense, Windows Server 2022.

2. Architecture du système

- Schéma réseau : présentation des interfaces, IPs, et connexions
- Explication de l'isolation des zones (LAN, DMZ, WAN)
- Rôle de chaque machine dans l'infrastructure



3. Préparation de l'environnement de travail dans VMware

- Installation de VMware Workstation
- Création d'une VM pour Proxmox avec un disque dur étendu
- Configuration de trois cartes réseau :
 - **WAN** (Bridge vers l'accès internet)
 - **LAN** (réseau interne pour le serveur Web LAN)
 - **DMZ** (réseau intermédiaire isolé pour le serveur Web DMZ)

4. Création et configuration des machines virtuelles

4.1. Création de la VM pfSense

- Téléchargement et installation de pfSense

Apres avoir lancer la vm en clique sur une suite de clique sur <<Suivant>> jusqu'à le telechargement suivant .



- Affectation des interfaces réseau (WAN / LAN / DMZ)

The image contains three side-by-side screenshots of the 'Virtual Machine Settings' window from a hypervisor interface, specifically focusing on the 'Network connection' tab.

- VM 1 (Left):** The 'LAN segment:' dropdown is set to 'LAN' and is highlighted with an orange box.
- VM 2 (Middle):** The 'LAN segment:' dropdown is set to 'DMZ' and is highlighted with an orange box.
- VM 3 (Right):** The 'LAN segment:' dropdown is set to 'DMZ' and is highlighted with an orange box.

In all three cases, the 'Network connection' section includes the following options:

- Bridged: Connected directly to the physical network (selected)
- Replicate physical network connection state
- NAT: Used to share the host's IP address
- Host-only: A private network shared with the host
- Custom: Specific virtual network

Configuration IP de base

Configure maintenant le LAN :

- Retour au menu → 2) Set interface(s) IP address → Choisis 2 - LAN.
- Saisis : IPv4 Address: 192.168.100.1/24

Configure maintenant le LAN :

- Retour au menu → 2) Set interface(s) IP address → Choisis 3 – OPT1.
- Saisis : IPv4 Address: 192.168.200.1/24

```
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 192.168.200.1/24
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 35710c216d10ba293b3'

*** Welcome to pfSense 2.6.0-RELEASE (arm64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 193.168.1.60/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.200.1/24

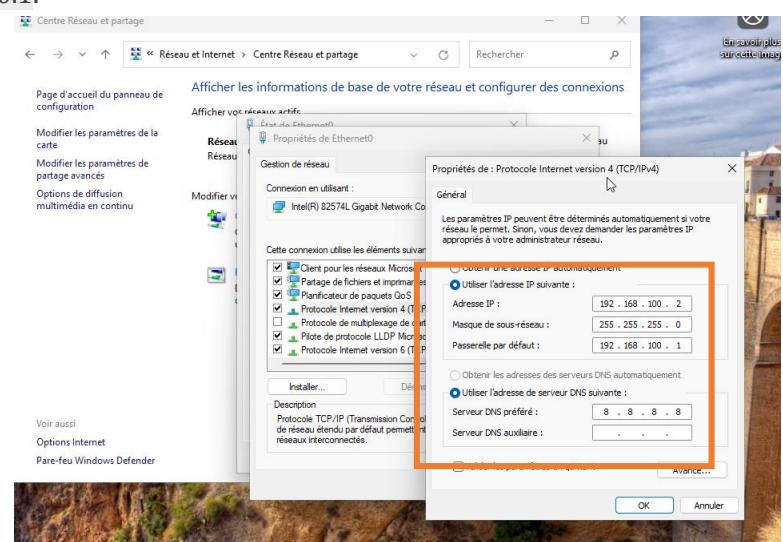
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14)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

Enter an option: ■
```

4.2. Création des deux serveurs Web

Serveur Web 1 (connecté au LAN)

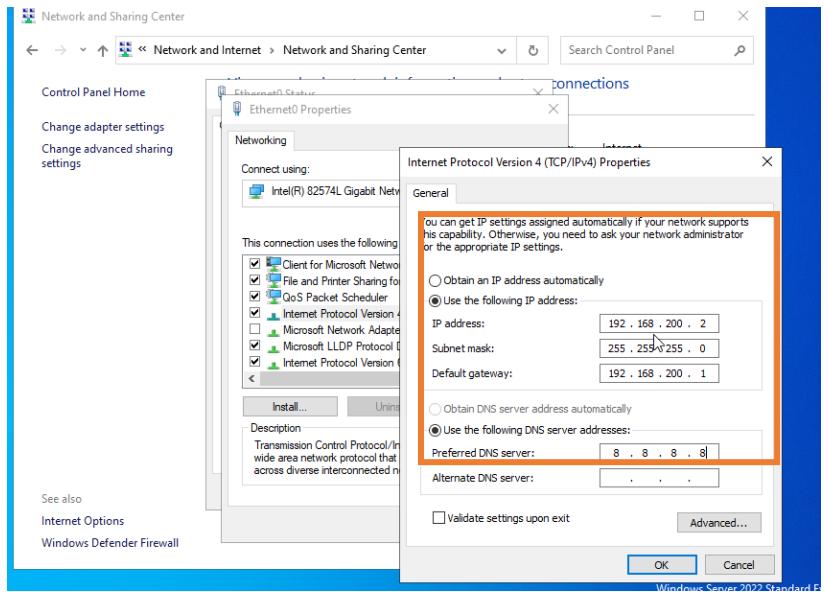
- Configuration IP dans le réseau LAN
 - IP : 192.168.100.2/24.
 - Passerelle : 192.168.100.1.



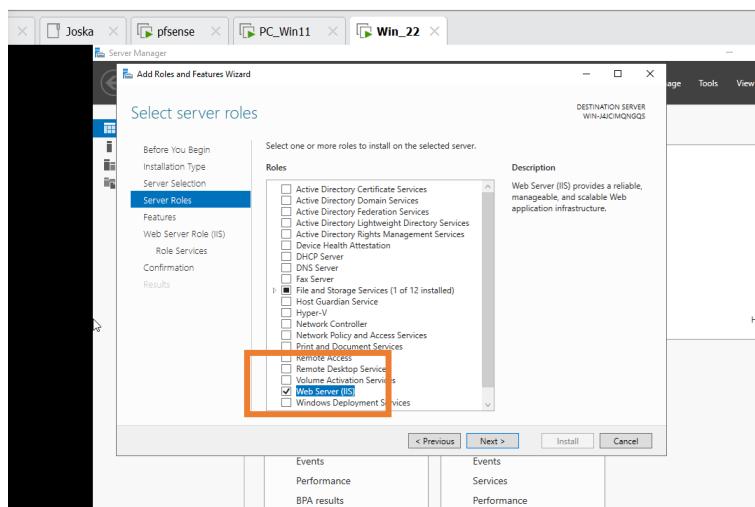
Serveur Web 2 (connecté à la DMZ)

- Installation similaire
- Configuration IP dans le réseau DMZ

- IP : 192.168.200.2/24.
- Passerelle : 192.168.200.1

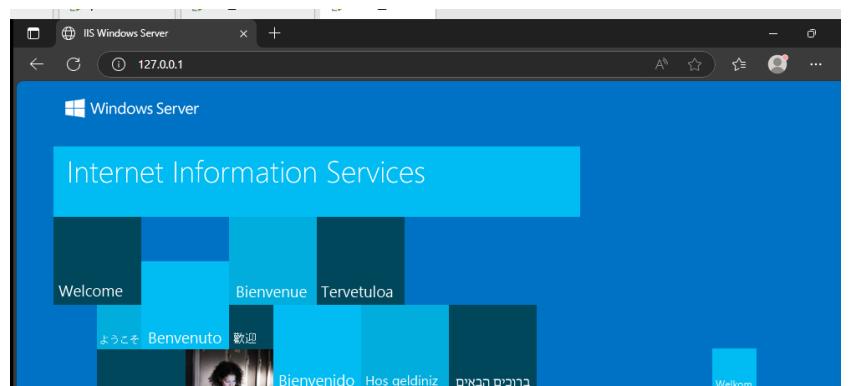


Installation des Roles IIS sur les deux Serveur :



- Vérification :

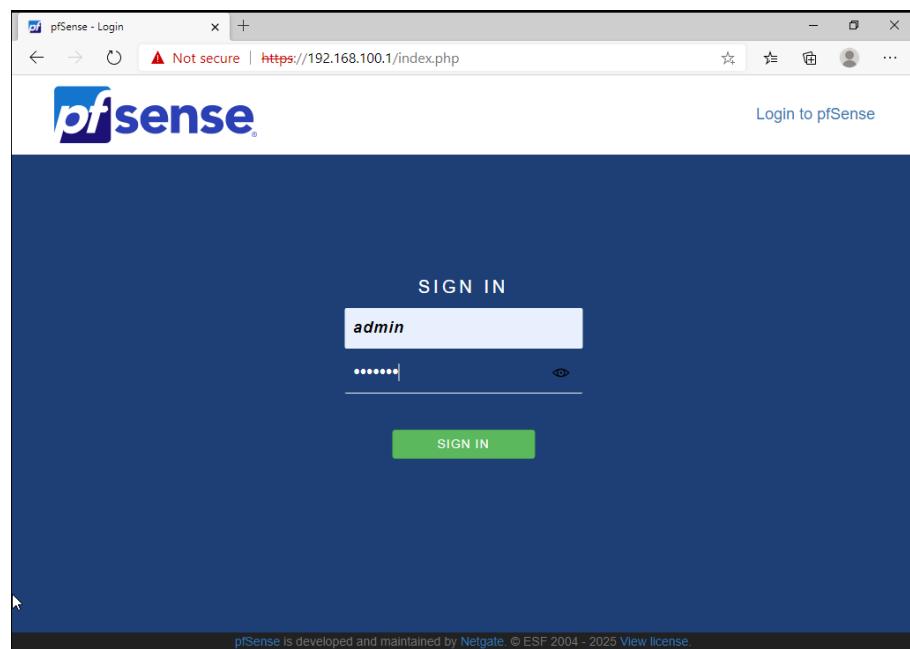
Accès à <http://127.0.0.1> interface par defaut de IIS



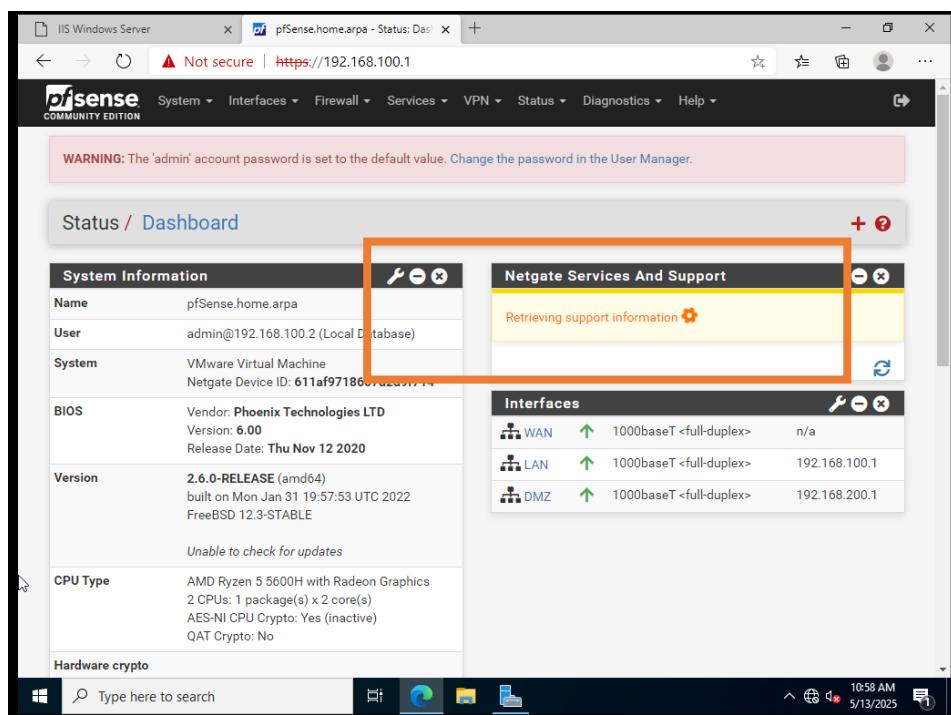
5. Configuration des composants

5.1 Accès à l'interface web :

- Branche un PC sur le même réseau que le LAN (192.168.1.0/24).
- **URL** : <https://192.168.100.1> (depuis le serveur LAN).
- **Identifiants** : admin/pfsense.



5.2. Présentation de l'Interface



- **Dashboard** : Vue globale du trafic, interfaces, état du firewall.
- **Menu principal** : Firewall, NAT, VPN, Services.

5.3. Règles de Pare-feu

- **LAN → DMZ** :

-Bloquer tout les paquets qui viennent de LAN a destination DMZ tout flux sera bloquer sera realiser comme suivant :

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

Edit Firewall Rule

Action: **Block** (boxed)

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: **LAN**
Choose the interface from which packets must come to match this rule.

Address Family: **IPv4**
Select the Internet Protocol version this rule applies to.

Protocol: **Any**
Choose which IP protocol this rule should match.

mercredi 7 mai 2025
mer. 05:08 (Heure locale)

Non sécurisé | https://192.168.100.1/firewall_rules_edit.php?if=lan&after=-1

Protocol: Any
Choose which IP protocol this rule should match.

Source
Source: Invert match **LAN net** (boxed)
Source Address /

Destination
Destination: Invert match **DMZ net** (boxed)
Destination Address /

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description: Bloquage des flux entre LAN et DMZ
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: [Display Advanced](#)

Save

PfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN DMZ

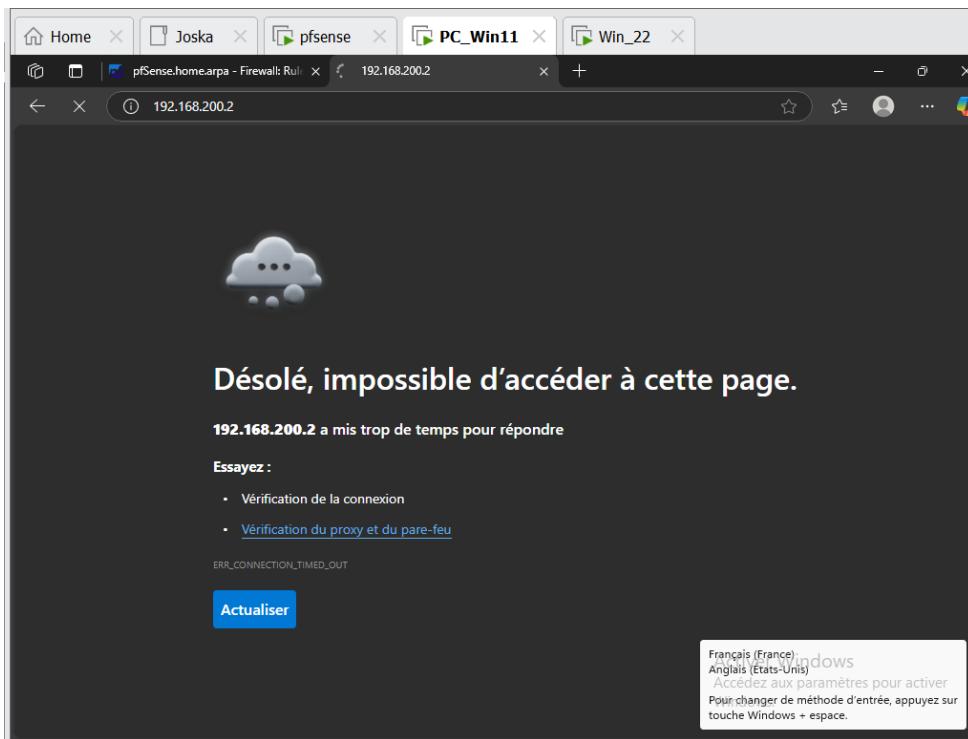
Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 3 /2.72 MIB	*	*	*	LAN Address	443 *	*	*		Anti-Lockout Rule	
✗ 0 /0 B	IPv4 *	LAN net	*	DMZ net	*	*	none		Bloquage des flux entre LAN et DMZ	
✗ ✓ 28 /1.09 MIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✗ ✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save

Haut-parleurs (High Definition Audio Device): 67%

Résultat :

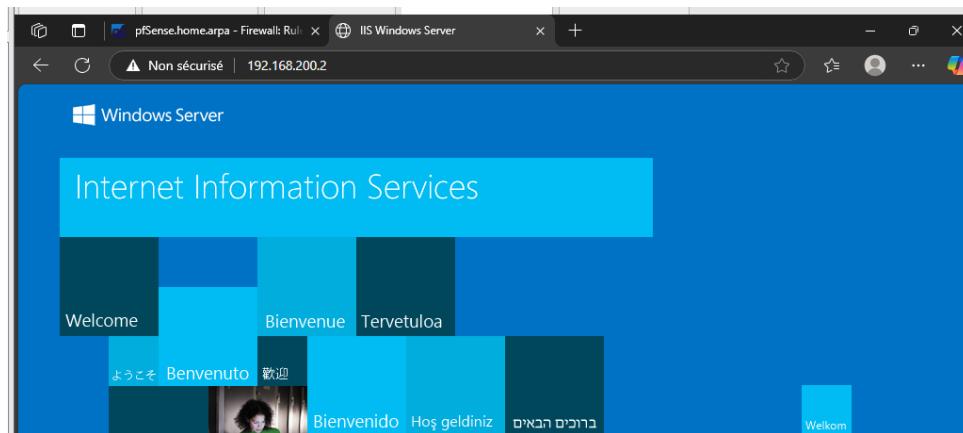


-Autoriser tout les paquets qui viennent de LAN a destination ServerWeb 192.168.200.2
 (http port 80) tout flux sera autoriser, qui sera realiser comme suivant :

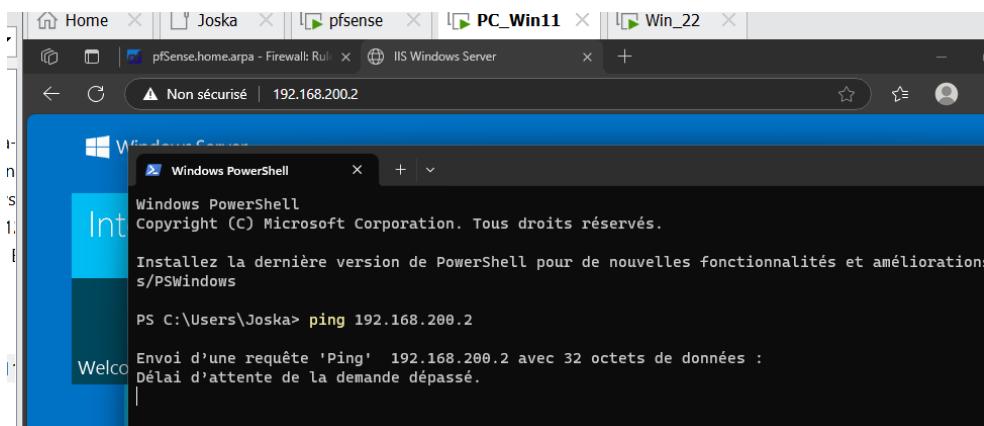
The screenshot shows the 'Edit Firewall Rule' page. The 'Action' dropdown is set to 'Pass' (highlighted with an orange box). The 'Source' section shows 'Source' set to 'LAN net' (highlighted with an orange box). Other settings include 'Address Family' (IPv4), 'Protocol' (TCP), and various checkboxes like 'Disabled' and 'Invert match'.

The screenshot shows the 'Edit Firewall Rule' page with the 'Destination' section active. The 'Destination' dropdown is set to 'Single host or alias' with '192.168.200.2' selected (highlighted with an orange box). The 'Destination Port Range' fields show 'From' as 'HTTP (80)' and 'To' as 'HTTP (80)'. The 'Extra Options' section includes a 'Log' checkbox (unchecked) and a 'Description' field containing 'ion acces serveur Web depuis LAN et sur le port 80 HTTP'. A 'Save' button is at the bottom.

Resultat :



-Si on réalise le ping vers le Serveur Web il ne va pas fonctionné



- **DMZ → LAN :**

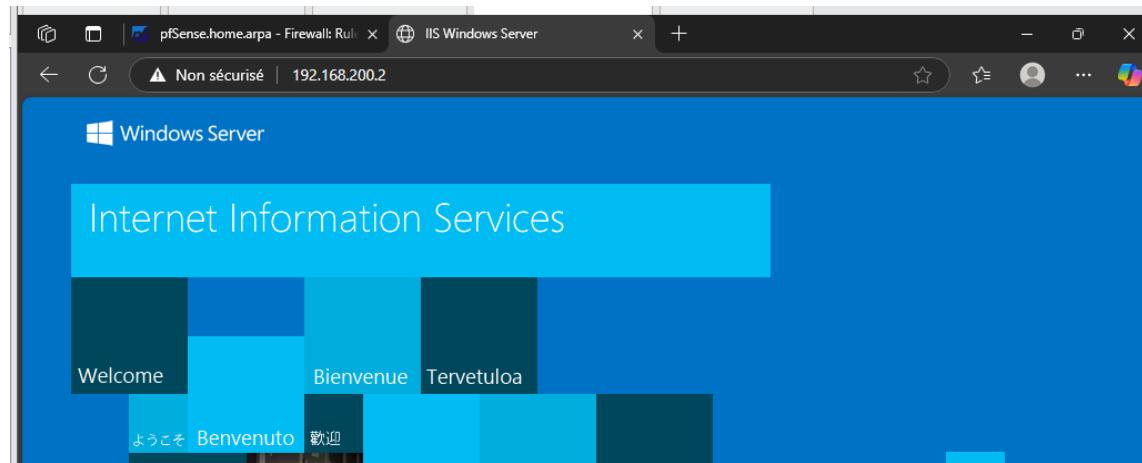
A screenshot of the pfSense Firewall Rules configuration interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. A warning message in a pink box says: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main area is titled 'Firewall / Rules / Edit'. A specific rule is selected for editing, with its 'Action' set to 'Block'. The 'Source' tab is visible at the bottom of the configuration pane.

- Bloquer tout trafic de source DMZ à destination LAN.

Choose which IP protocol this rule should match.

Source	<input type="checkbox"/> Invert match	DMZ net	Source Address	/	▼
Destination	<input type="checkbox"/> Invert match	LAN net	Destination Address	/	▼
Extra Options					
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).				
Description	Bloquage des flux vers LAN				
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.					
Advanced Options	Display Advanced				
Rule Information					
Tracking ID	1746586827				
Created	5/7/25 05:00:27 by admin@192.168.100.2 (Local Database)				
Updated	5/7/25 05:01:16 by admin@192.168.100.2 (Local Database)				
Save					

Résultat :



Autoriser la DMZ à accéder à Internet

The screenshot shows the pfSense Firewall Rules Edit interface. A specific rule is being configured:

- Action:** Pass (highlighted with an orange box)
- Disabled:** Disable this rule
- Interface:** DMZ
- Address Family:** IPv4
- Protocol:** TCP
- Source:** DMZ net (highlighted with an orange box)
- Destination:** any (highlighted with an orange box), Destination Port Range: HTTPS (443) (highlighted with an orange box)
- Extra Options:**
 - Log:** Log packets that are handled by this rule
 - Description:** (empty field)
 - Advanced Options:** Display Advanced

Réultat : Accès à Internet sera autorisé Avec l'ensemble de règle créée

The screenshot shows a web browser window with two tabs. The top tab is titled "pfSense.home.arpa - Firewall: Rules" and the bottom tab is also titled "pfSense.home.arpa - Firewall: Rules". The main content area displays the "Firewall / Rules / DMZ" interface. A red box highlights the second rule in the list, which is a TCP rule allowing port 443 (HTTPS) from the DMZ network to the LAN network.

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		Bloquage des flux vers LAN	
0 / 0 B	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	none			
3 / 116 Kib	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	none			
0 / 0 B	IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	none			

At the bottom of the interface, there are buttons for "Add" (green), "Delete" (red), "Save" (blue), and "Separator" (orange).

-Ajout d'une règle NAT qui autorise les flux de l'interface WAN (http)

The screenshot shows the 'Edit Redirect Entry' configuration page in the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main form is titled 'Edit Redirect Entry' and contains the following fields:

- Disabled:** Disable this rule
- No RDR (NOT):** Disable redirection for traffic matching this rule. A note below says: 'This option is rarely needed. Don't use this without thorough knowledge of the implications.'
- Interface:** WAN (dropdown menu)
Choose which interface this rule applies to. In most cases "WAN" is specified.
- Address Family:** IPv4 (dropdown menu)
Select the Internet Protocol version this rule applies to.
- Protocol:** TCP (dropdown menu)
Choose which protocol this rule should match. In most cases "TCP" is specified.
- Source:**
- Destination:** Invert match.
Type: WAN address
Address/mask:
Range: From port: To port:
Note: Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
- Redirect target IP:** Type: Single host Address: 192.168.200.2
Note: Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (::1)
- Redirect target port:** Port: HTTP
Custom
Note: Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.
- Description:**
A description may be entered here for administrative reference (not parsed).
- No XMLRPC Sync:** Do not automatically sync to other CARP members
Note: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
- NAT reflection:** Use system default
- Filter rule association:** Rule NAT
[View the filter rule](#)

Trester l'accès au serveur web à partir d'un réseau WAN

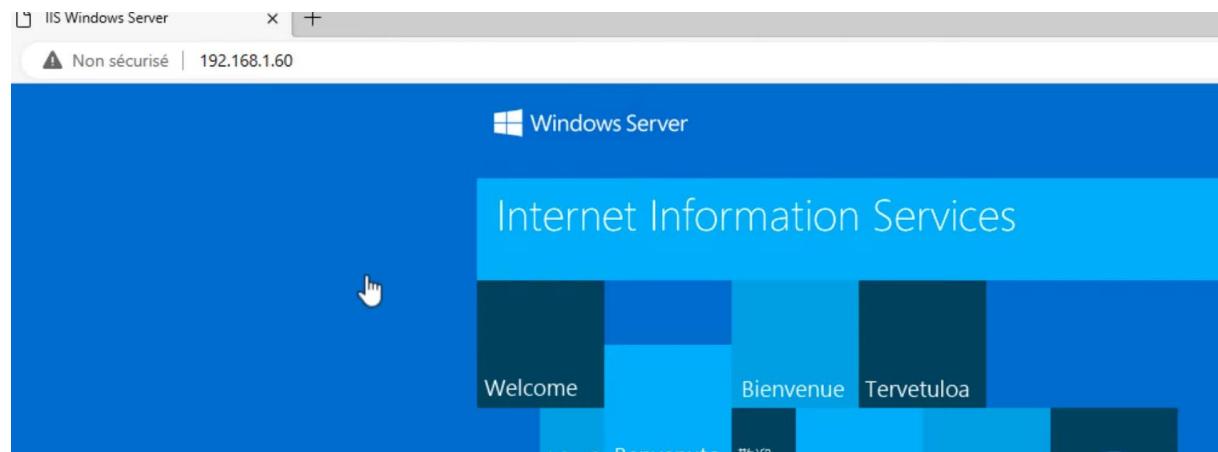
The screenshot shows the pfSense Firewall / NAT / Port Forward configuration page. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the header, the title "Firewall / NAT / Port Forward" is displayed. Under the title, there are tabs: Port Forward, 1:1, Outbound, and NPt. The Port Forward tab is selected. The main area is titled "Rules" and contains a table with columns: #, Interface, Protocol, Source Address, Source Ports, Dest. Address, Dest. Ports, NAT IP, NAT Port, Description, and Actions. One rule is listed: "WAN TCP * * WAN address 80 (HTTP) 192.168.200.2 80 (HTTP)". The "Actions" column for this rule includes edit, delete, and separator buttons. Below the table is a legend: "Pass" (represented by a green arrow icon) and "Linked rule" (represented by a crossed-link icon). At the bottom of the page are buttons for Add, Save, and Separator.

- **WAN:**

- Donner accès au serveur Web depuis WAN

The screenshot shows the pfSense Firewall & NAT settings page, specifically the "Reserved Networks" section. This section contains two options: "Block private networks and loopback addresses" (checkbox checked) and "Block bogon networks" (checkbox checked). The "Block private networks and loopback addresses" option is highlighted with an orange box. Below each option is a detailed description of its function. At the bottom of the page is a "Save" button.

Résultat :



Synthèse :

Les règles que nous avons créées jouent un rôle critique dans la sécurité et la fonctionnalité de votre DMZ virtuelle. Elles permettent :

1. **Contrôle d'accès** : Le firewall (pfSense) filtre le trafic entrant/sortant, autorisant uniquement les connexions nécessaires (ex: HTTP vers le serveur web).
2. **Isolation réseau** : Les règles isolent la DMZ du LAN interne, protégeant la base de données des accès directs depuis Internet.
3. **Redirection des flux** : Le NAT (Port Forwarding) guide le trafic externe vers le serveur web en DMZ, tout en masquant l'infrastructure interne.
4. **Journalisation** : Les logs des règles aident à détecter des intrusions ou anomalies.

En résumé, ces règles matérialisent notre architecture sécurisée, équilibrant accessibilité et protection.

Conclusion Générale

À travers ce projet, nous avons pu **modéliser une DMZ fonctionnelle**, mettant en œuvre :

- **Une isolation efficace** des services via pfSense, permettant d'exposer le serveur web tout en protégeant le serveur SQL des accès directs.
- **Une gestion fine des flux** grâce aux règles NAT et firewall, assurant à la fois accessibilité et sécurité.
- **Une approche pratique** de la virtualisation sous Proxmox, depuis le déploiement des VMs jusqu'à la configuration réseau avancée.

Cette expérience renforce l'importance d'une **architecture en couches** pour les infrastructures critiques, où chaque élément (pare-feu, serveurs, règles) joue un rôle précis dans la mitigation des risques. Les compétences acquises (routage, segmentation, gestion des accès) sont transposables à des environnements professionnels, cloud ou hybrides.