BTS SIO SISR — 2ème année

Rapport de TP

Atelier LAN, WAN et DMZ sur Proxmox VE

Nom / Prénom	Bricet Théo / Raphael ROSARIO
Classe / Groupe	BTS SIO / Option SISR
Date	30/09/2026
Contexte	Proxmox / TP

Partie A — Architecture et Topologie Réseau

Voici le schéma de l'architecture réseau globale, réalisé avec Draw.io.

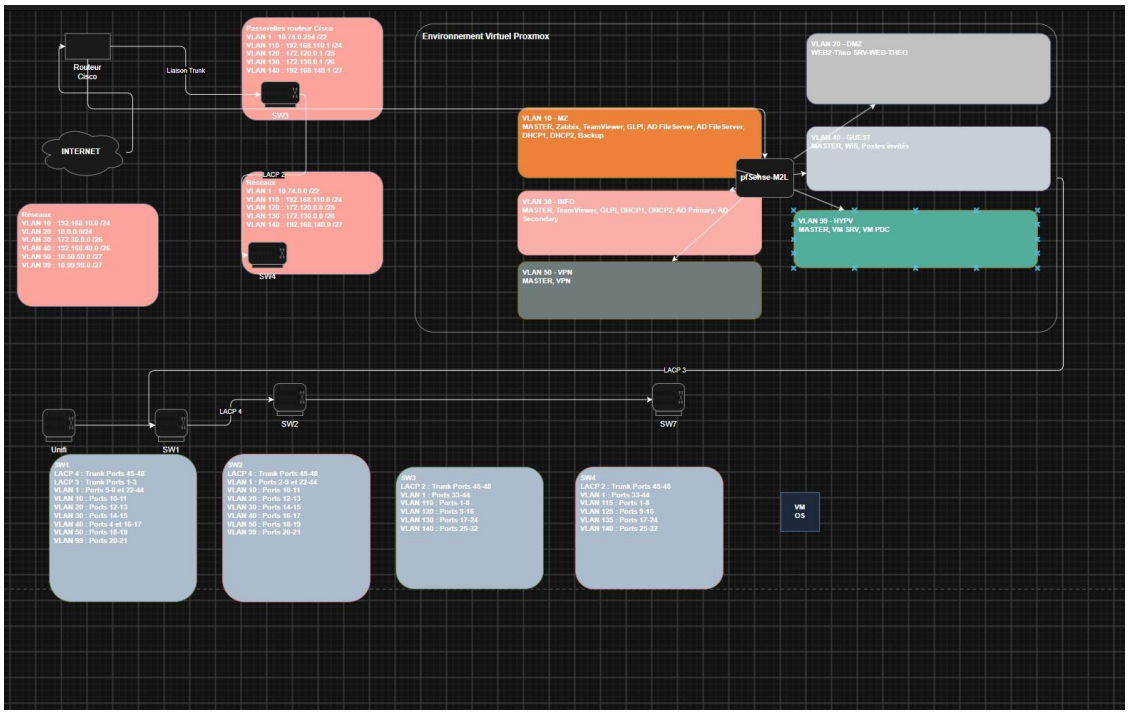


Figure 1 : *Schéma de l'architecture réseau globale (Draw.io)*

Plan d'adressage de la maquette :

Machine	Bridge	Adresse IP	Passerelle	Remarque
FW-Theo (WAN)	vmbr0	10.74.1.24/22	Fournie par l'atelier	Adresse obtenue en DHCP
FW-Theo (LAN)	vmbr1	192.168.10.1/24	—	DHCP de .100 à .150
FW-Theo (DMZ)	vmbr2	10.0.0.1/24	—	Interface OPT1 renommée DMZ
CLI-Theo	vmbr1	DHCP (192.168.10.100)	192.168.10.1	Windows 10
SRV-WEB-THEO	vmbr2	10.0.0.10/24	10.0.0.1	Debian
web2-theo (bonus)	vmbr2	10.0.0.11/24	10.0.0.1	Debian

Partie B — Proxmox

Avant d'installer les machines, j'ai vérifié les bridges sur le nœud Proxmox. vmbr1 (LAN) et vmbr2 (DMZ) sont créés sans port physique.

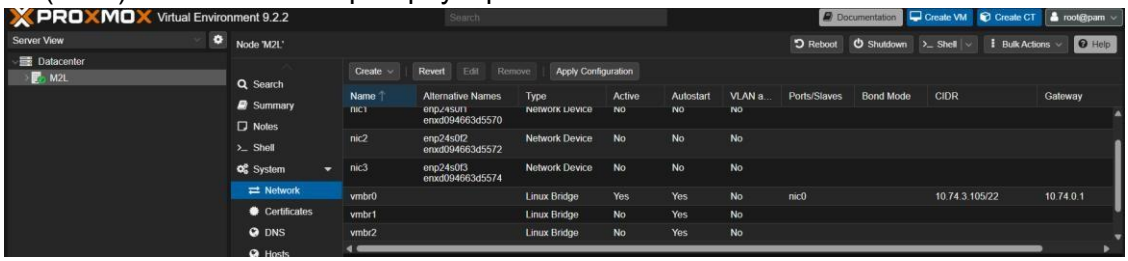


Figure 2 : *Onglet System > Network du nœud M2L avec vmbr0 (relié à nic0), vmbr1 et vmbr2*

Partie C — pfSense

Création de la VM du pare-feu, puis configuration des interfaces depuis la console.

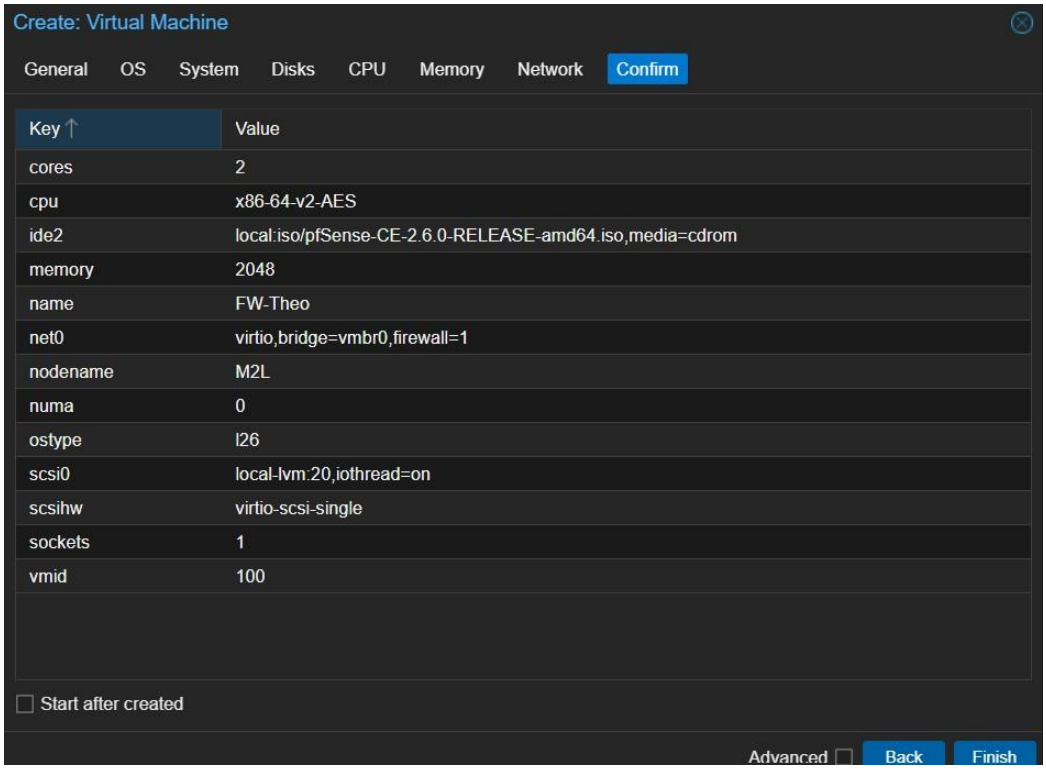


Figure 3 : *Récapitulatif de création de la VM FW-Theo (2 cœurs, 2 Go de RAM, ISO pfSense CE 2.6.0, disque de 20 Go)*



Figure 4 : *Console pfSense après l'assignation des interfaces (WAN sur vtnet0, LAN sur vtnet1, OPT1 sur vtnet2)*

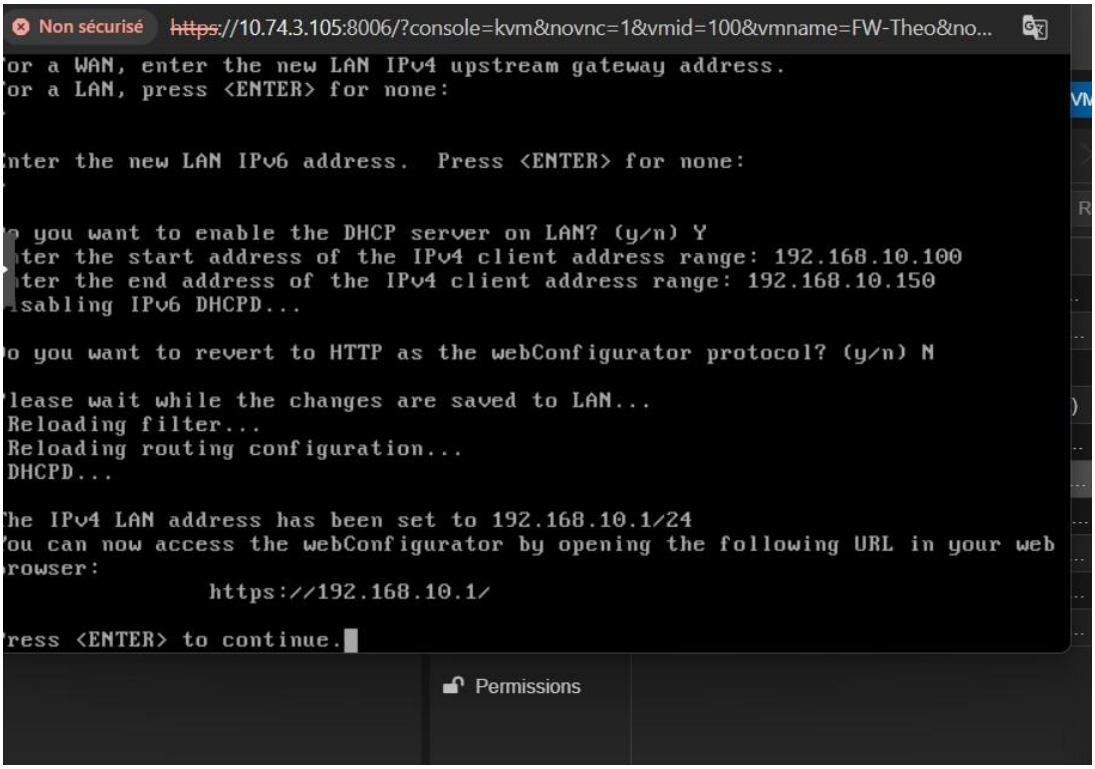


Figure 5 : *Configuration du LAN en 192.168.10.1/24 et activation du serveur DHCP (plage .100 à .150)*

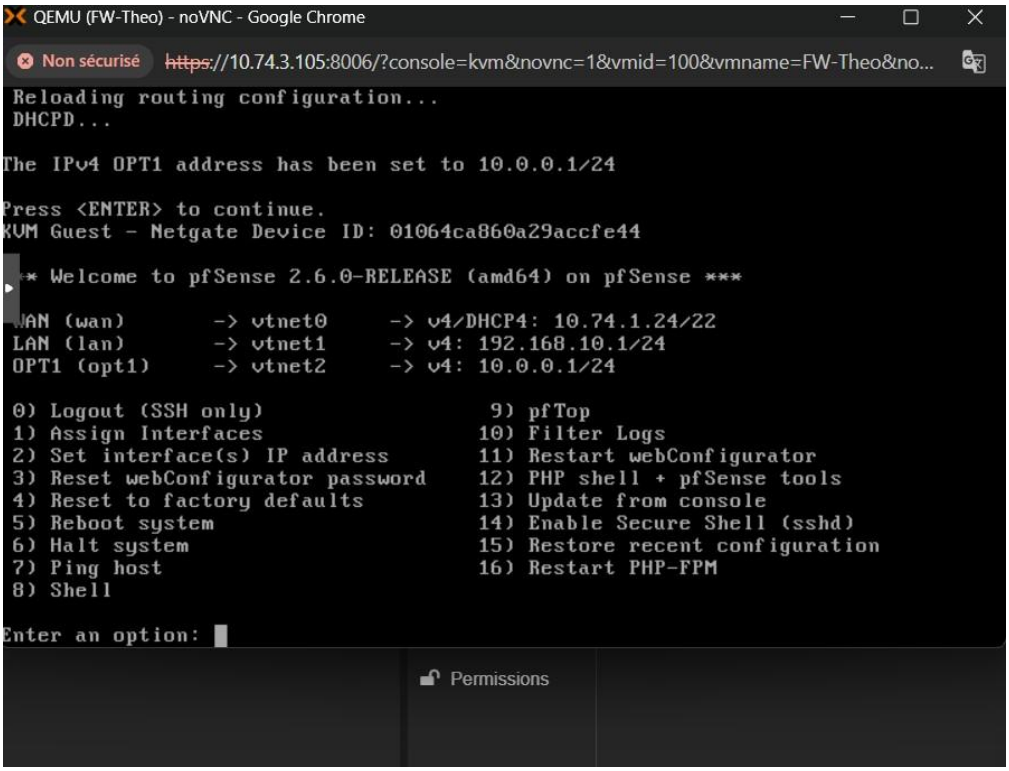


Figure 6 : *Console pfSense avec les trois interfaces configurées (WAN en DHCP, LAN 192.168.10.1/24, OPT1 10.0.0.1/24)*

Partie D — Client Windows

Création de la VM cliente dans le LAN, puis vérification de l'adresse reçue et de l'accès au pare-feu.

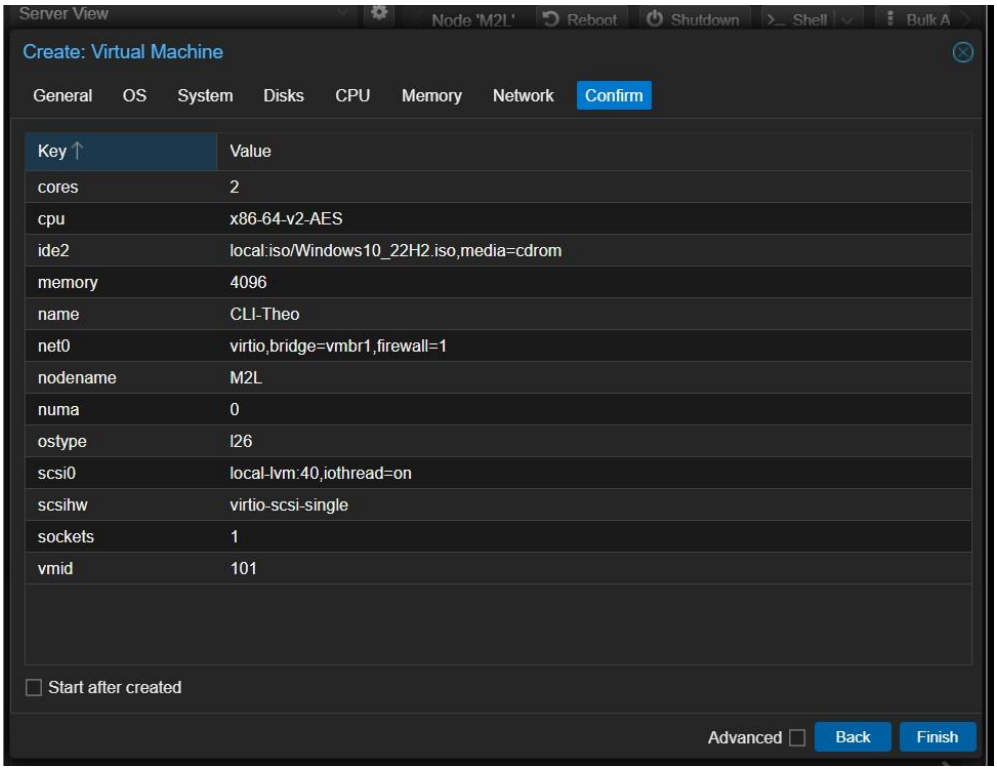


Figure 7 : *Récapitulatif de création de la VM CLI-Theo (Windows 10 22H2, 4 Go de RAM, carte réseau sur vmbr1)*

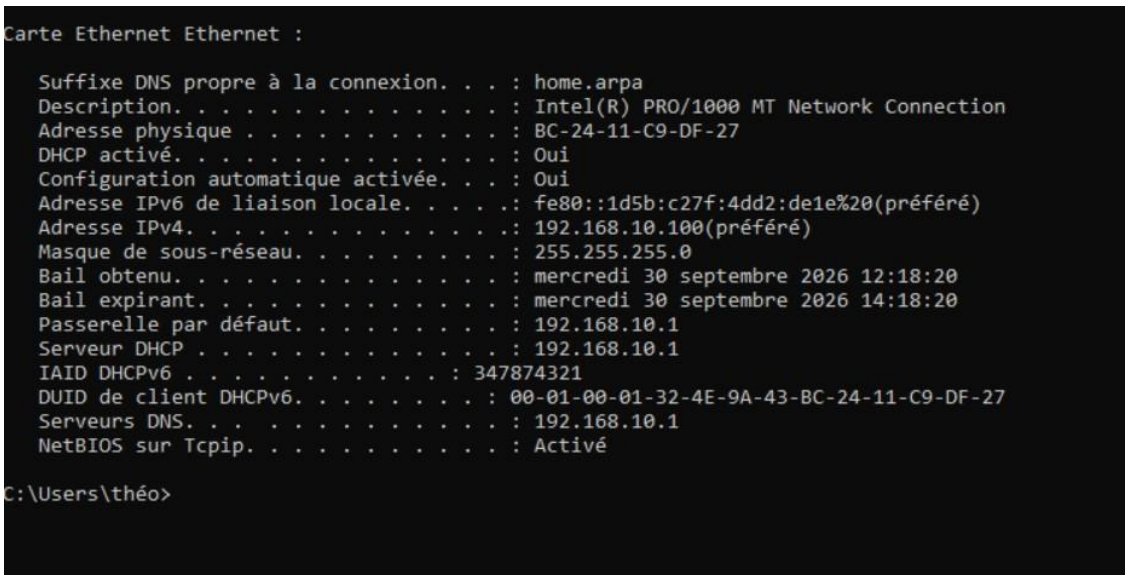


Figure 8 : *Résultat de ipconfig /all sur le client (IP 192.168.10.100 en DHCP, passerelle et serveur DHCP 192.168.10.1)*

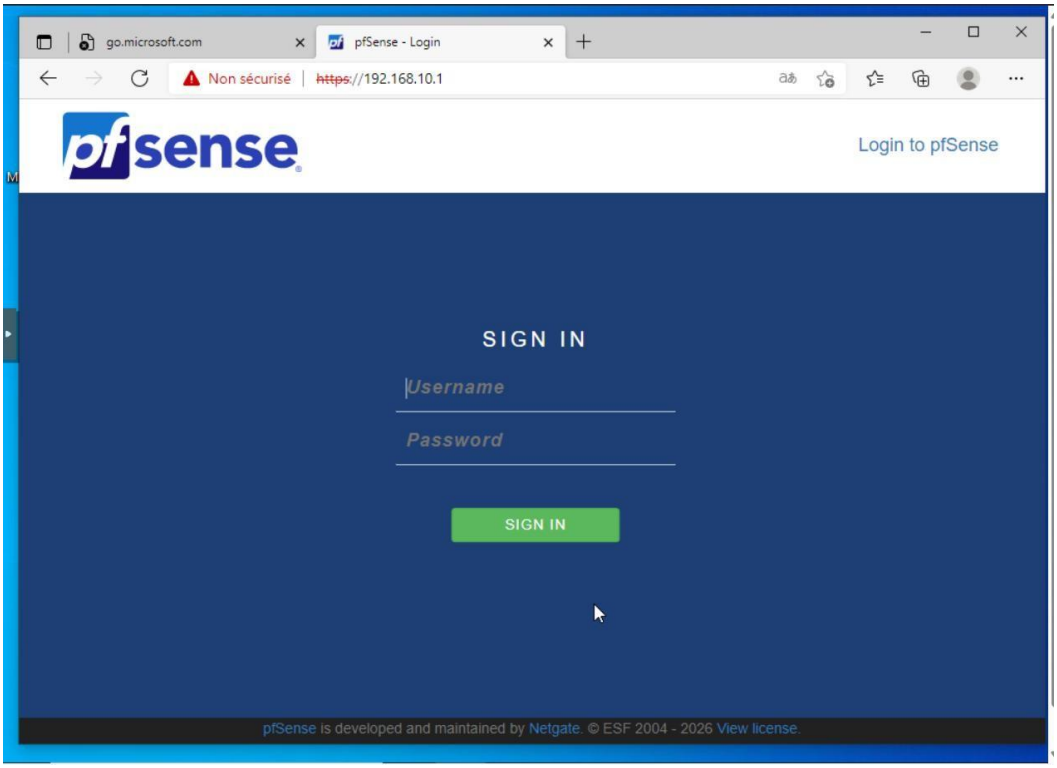


Figure 9 : *Page de connexion de pfSense ouverte depuis le client sur https://192.168.10.1*

Partie E — Admin & DMZ

Depuis le client, je me suis connecté à l'interface d'administration pour renommer le parefeu, configurer la DMZ et vérifier ses règles.

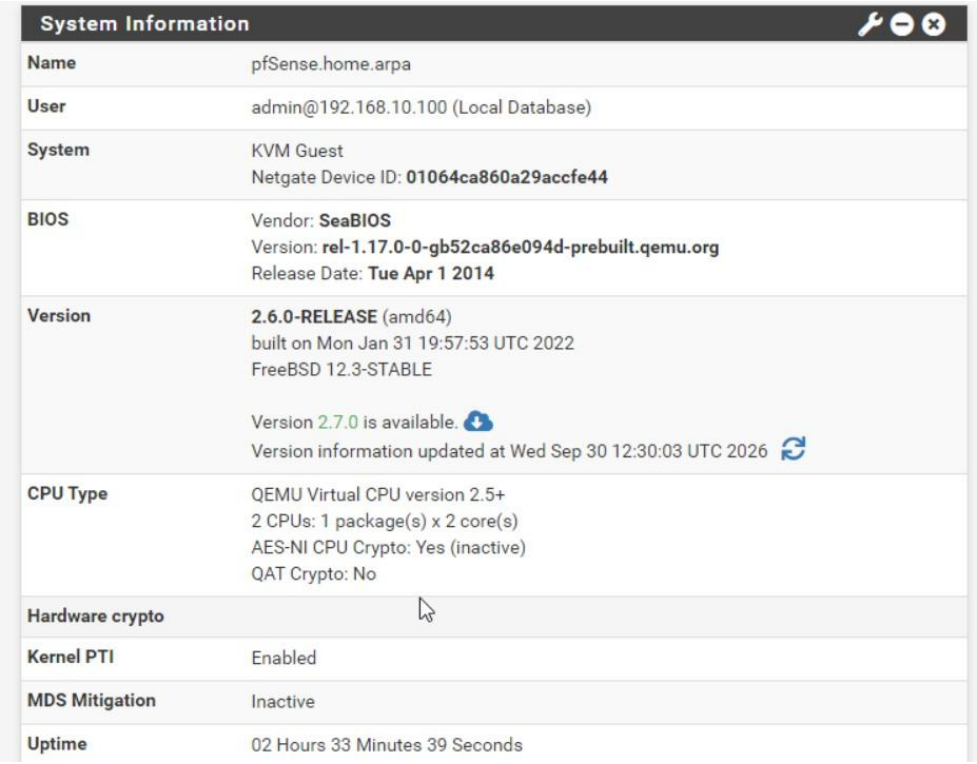


Figure 10 : *Tableau de bord pfSense (System Information) consulté depuis le client avec le compte admin*

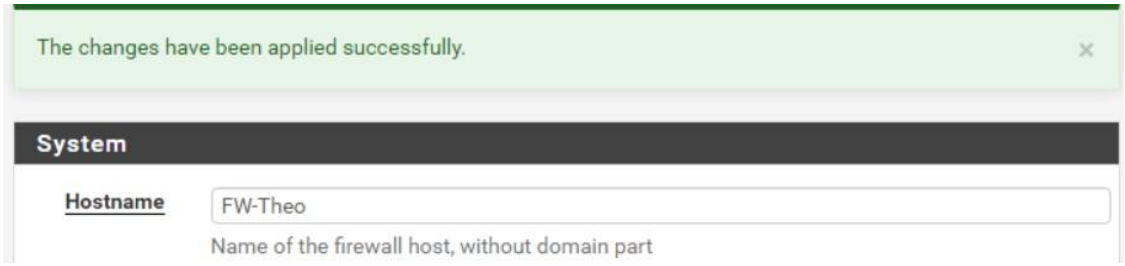


Figure 11 : *Nom d'hôte du pare-feu changé en FW-Theo, modification appliquée*



Figure 12 : *Interface OPT1 activée et renommée DMZ*

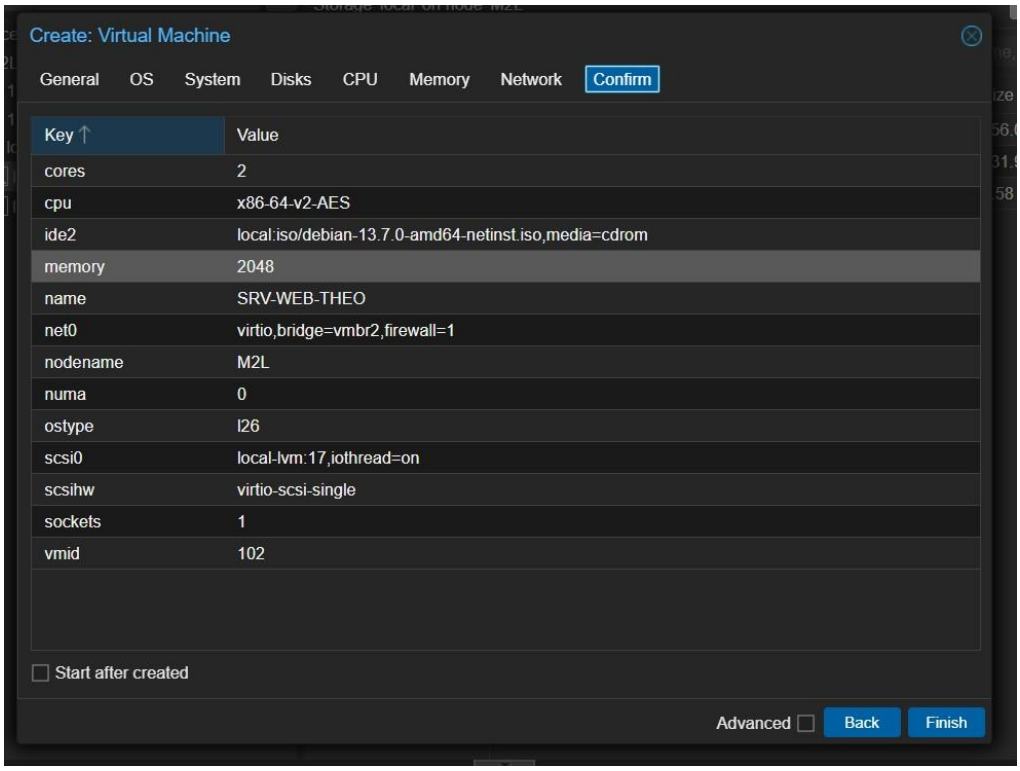


Figure 13 : *Liste des règles de l'interface DMZ*

Partie F — Serveur Web

Création du serveur web dans la DMZ, configuration de son IP fixe, puis test depuis le client.

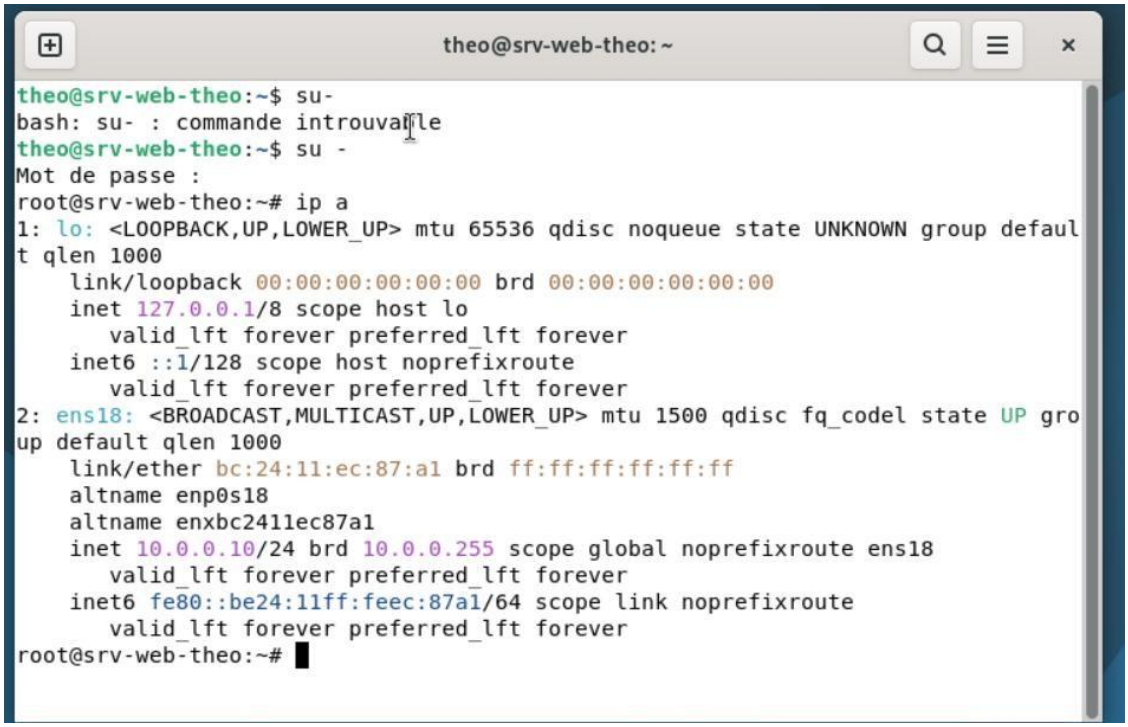


Figure 14 : *Récapitulatif de création de la VM SRV-WEB-THEO (Debian, 2 Go de RAM, carte réseau sur vmbr2)*

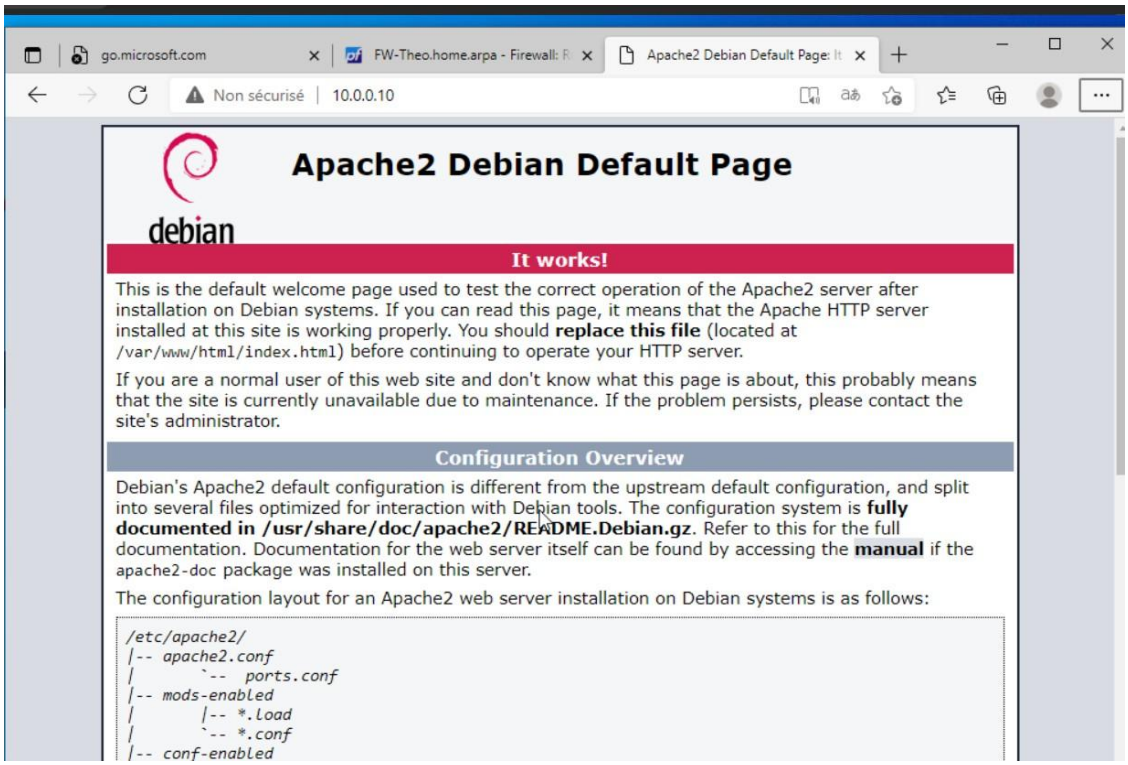


Figure 15 : *Résultat de ip a sur le serveur web (interface ens18 en 10.0.0.10/24)*



Figure 16 : *Page par défaut du serveur web affichée depuis le client sur http://10.0.0.10*

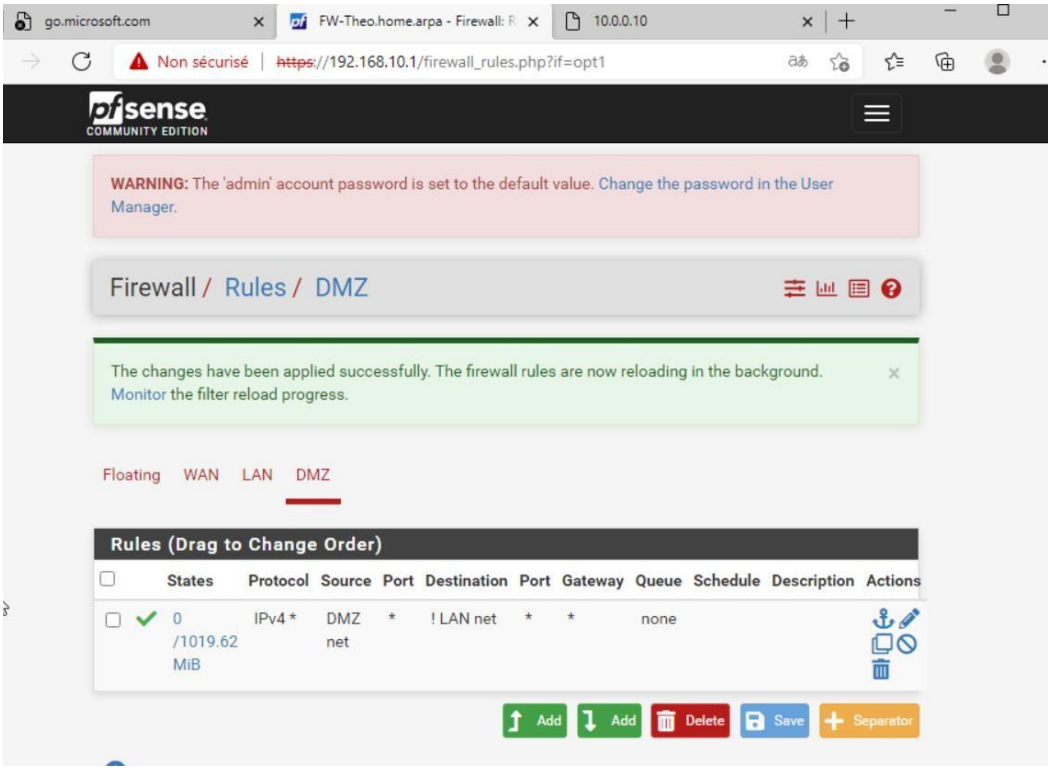


Figure 17 : *Page d'accueil personnalisée du serveur web affichée depuis le client*

Partie G — Questions de compréhension

Question 1

Quel est l'intérêt de placer le serveur web en DMZ plutôt que dans le LAN ? Quel risque évite-t-on ?

On met le serveur web en DMZ parce qu'il est ouvert sur Internet. Ça permet de le séparer de nos ordinateurs du LAN. Si un pirate réussit à pirater le serveur web, il reste bloqué dans la DMZ et ne peut pas accéder à nos ordinateurs ni à nos données dans le LAN.

Question 2

Quelle est la différence entre la redirection de port (NAT) et la règle de filtrage ? Pourquoi faut-il les deux ?

La redirection de port (NAT) sert à envoyer le trafic qui arrive sur l'IP du pare-feu vers l'IP du serveur web (10.0.0.10).

La règle de filtrage sert à dire au pare-feu d'autoriser ou de bloquer ce trafic.

Il faut les deux parce que le NAT donne la bonne adresse au paquet, et la règle de filtrage lui donne l'autorisation de passer.

Question 3

Pourquoi a-t-on décoché Block private networks sur le WAN en laboratoire ? Que faudrait-il faire en production ?

En cours/labo, notre réseau WAN utilise des adresses IP privées (du type 10.74.x.x). Si on laisse cette option cochée, le pare-feu bloque tout.

En vraie entreprise (production), il faut la cocher pour bloquer les fausses adresses IP qui viendraient d'Internet.

Question 4

Pourquoi la règle Block LAN → DMZ est-elle placée après la règle Pass vers le serveur web ?

Le pare-feu lit les règles de haut en bas et s'arrête à la première qui correspond.

On met la règle Pass en premier pour autoriser l'accès au serveur web. Ensuite, la règle Block en dessous bloque tout le reste des accès vers la DMZ.

Partie H — Bonus (Deuxième serveur web & SSL)

Pour le bonus, j'ai créé un deuxième serveur web dans la DMZ (WEB2) et configuré son adresse IP fixe.

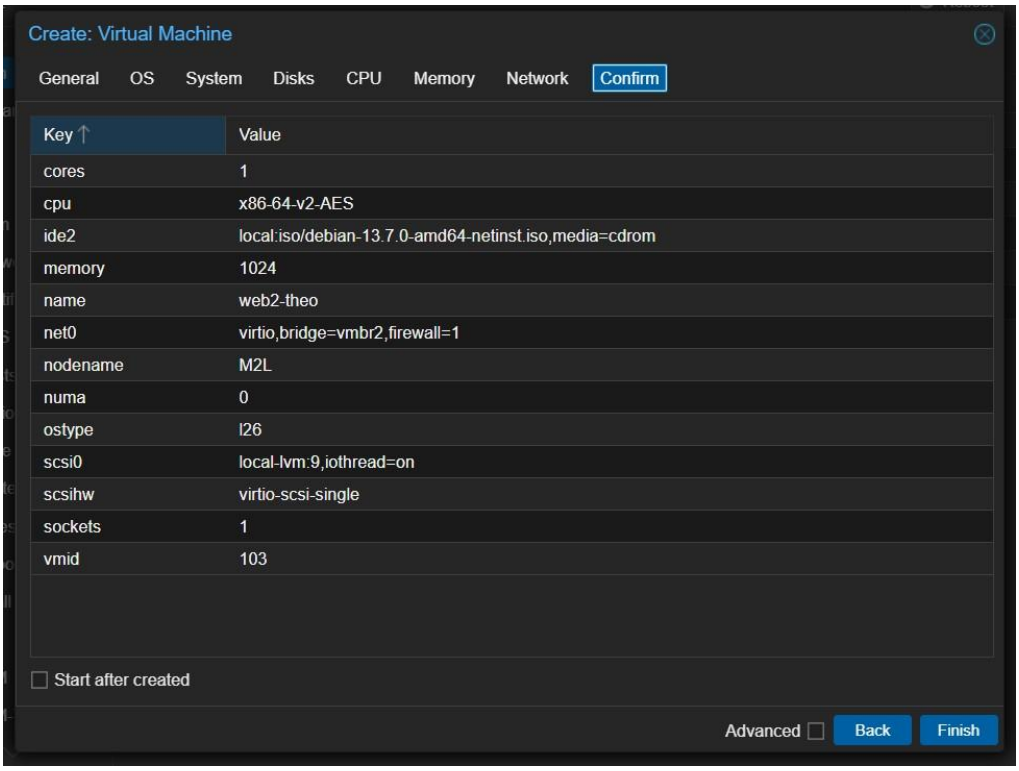


Figure 18 : *Récapitulatif de création de la VM web2-theo (Debian, 1 Go de RAM, carte réseau sur vmbr2)*

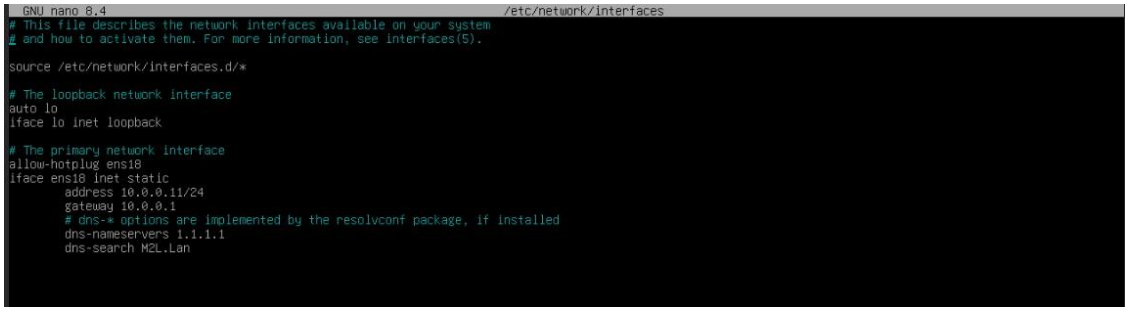


Figure 19 : *Fichier /etc/network/interfaces de WEB2 (IP statique 10.0.0.11/24, passerelle 10.0.0.1, DNS 1.1.1.1)*

Question bonus (H7)

Pourquoi le navigateur affiche-t-il un avertissement avec ce certificat ? Que faudrait-il utiliser pour un site public ?

Le navigateur affiche une alerte parce que le certificat est auto-signé (créé par nousmêmes). Comme il n'est pas validé par une vraie autorité de confiance (comme Let's Encrypt), le navigateur prévient que le site n'est pas certifié.

Pour un vrai site sur Internet, il faut utiliser un vrai certificat délivré par une autorité officielle comme Let's Encrypt.