LE DMZ, MISE EN PLACE ET SECURISATION

BTS S.I.O. OPTION S.I.S.R. -- 2025 - 2026

MR MICHELE MASTROGIACOMO

Introduction

J'ai réalisé un TP portant sur la mise en place d'une DMZ (Zone Démilitarisée) au sein de mon infrastructure réseau.

Ce TP s'appuie sur mon PPE principal, qui est segmenté en plusieurs réseaux (LAN utilisateurs, serveurs, Wi-Fi et DMZ).

L'objectif est de sécuriser l'accès aux services exposés sur Internet, notamment un serveur Web et un serveur SFTP, tout en protégeant le réseau interne.

Le DMZ, c'est une zone protégée, qui ne communique pas directement dans Lan local de l'infrastructure mais son serveur WEB et SFTP devient accessible pour l'utilisateur du Lan seulement travers Internet.

Cette solution est mise en place pour une sécurité majeure, le serveur web est le service plus expose aux attaques informatiques et aux exploitations, donc si tombe en panne ou prise de cible par des attaquant le dégât reste uniquement dans le serveur même car des règles de filtrage ont été mis en place pour éviter une propagation des éventuelles attaques.

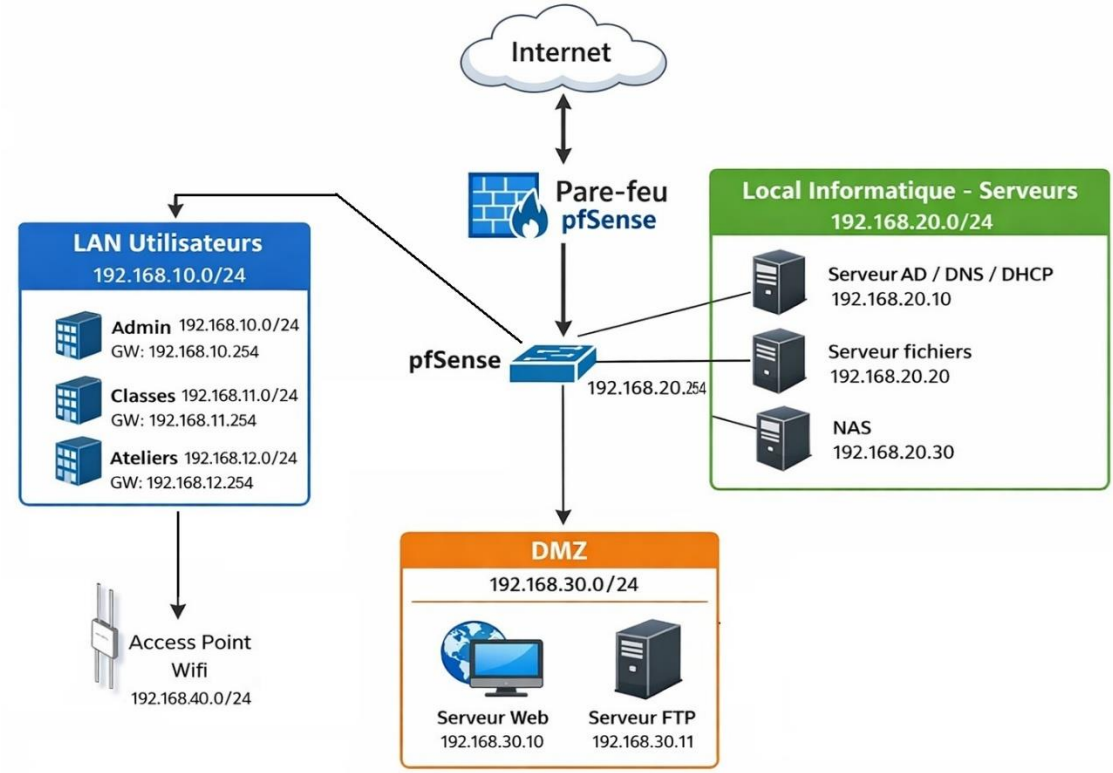
Contexte et présentation de l'infrastructure

L'infrastructure réseau est segmentée en plusieurs sous-réseaux :

- Réseau utilisateurs (192.168.10.0/24, 11.0/24, 12.0/24)
- Réseau serveurs (192.168.20.0/24)
- Réseau DMZ (192.168.30.0/24)
- Réseau Wi-Fi (192.168.40.0/24)

Le pare-feu pfSense assure le routage et la sécurité entre ces différents réseaux ainsi que l'accès à Internet.

Image 1 : Schema segmentation réseau



Objectifs de la DMZ

Ce DMZ a été étudié pour une utilisation là où le données personnelles et la sécurité du système d'information doit être optimale. Le contexte d'un périmètre scolaire et la différente présence d'utilisateur on besoin d'une sécurisation majeure.

La mise en place d'une DMZ permet :

- d'isoler les services accessibles depuis Internet
- de limiter les risques d'intrusion vers le réseau interne
- de contrôler précisément les flux réseau grâce aux règles de pare-feu

Dans ce TP, la DMZ héberge :

- un serveur Web avec OS Lubuntu (192.168.30.10)
- un serveur SFTP ave Debian sans GUI (192.168.30.11)

Mise en place technique

Création de la DMZ dans pfSense

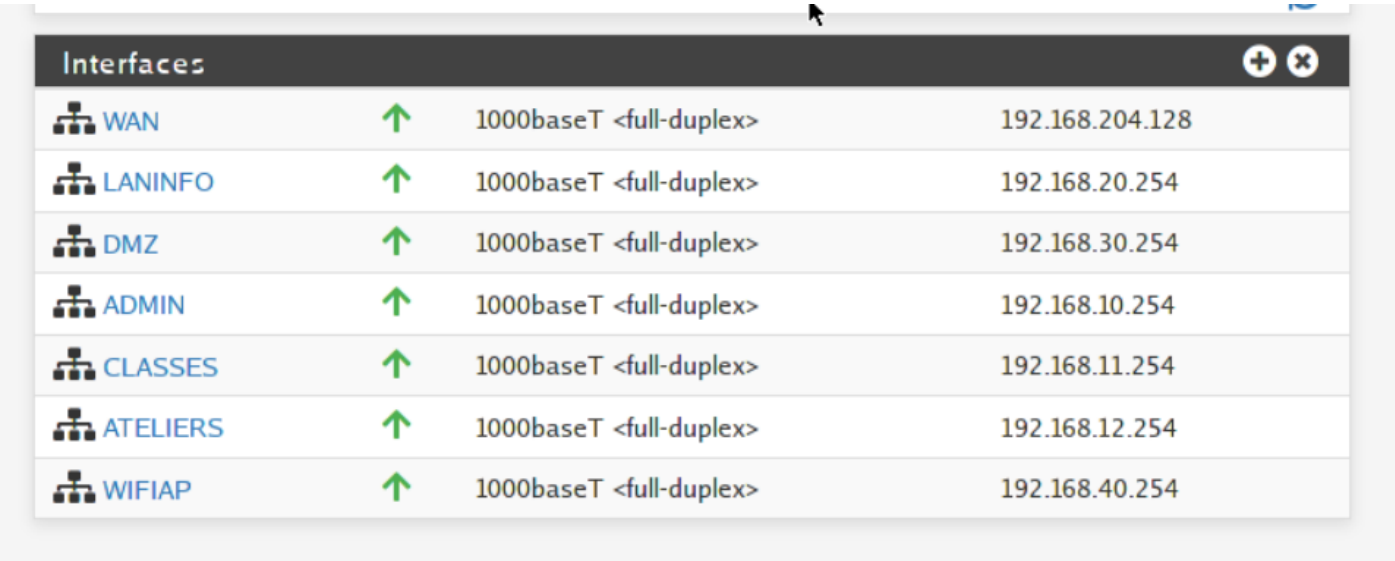
Comme première tâche une interface DMZ a été créée dans pfSense avec les paramètres suivants :

- Adresse réseau : 192.168.30.0/24
- Passerelle : 192.168.30.254

Cette interface permet de séparer logiquement les serveurs exposés du reste du réseau interne.

Une adresse IP a été attribuée à l'interface DMZ (192.168.30.254), qui sert de passerelle pour les machines présentes dans cette zone. Chaque réseau possède sa propre passerelle pour une meilleure gestion de flux réseaux et des réglages.

Image 2 : Interfaces pfSense (avec DMZ)



Configuration des serveurs

Deux serveurs ont été déployés dans la DMZ :
Serveur Web sous Lubuntu :

- IP : 192.168.30.10
- Service : HTTP (port 80)

Serveur SFTP sous Debian sans GUI :

- IP : 192.168.30.11
- Service : SFTP (port 22)

Chaque serveur a été configuré avec une adresse IP fixe dans le réseau DMZ afin de garantir une accessibilité stable. Ces serveurs sont accessibles uniquement selon les règles définies dans le pare-feu. Les services ont ensuite été installés et activés :

- Sur le serveur web : Apache
- Sur le serveur SFTP : via SSH

Image 3 : IP du serveur Web avec résolution du DNS (AD dans un autre réseau)

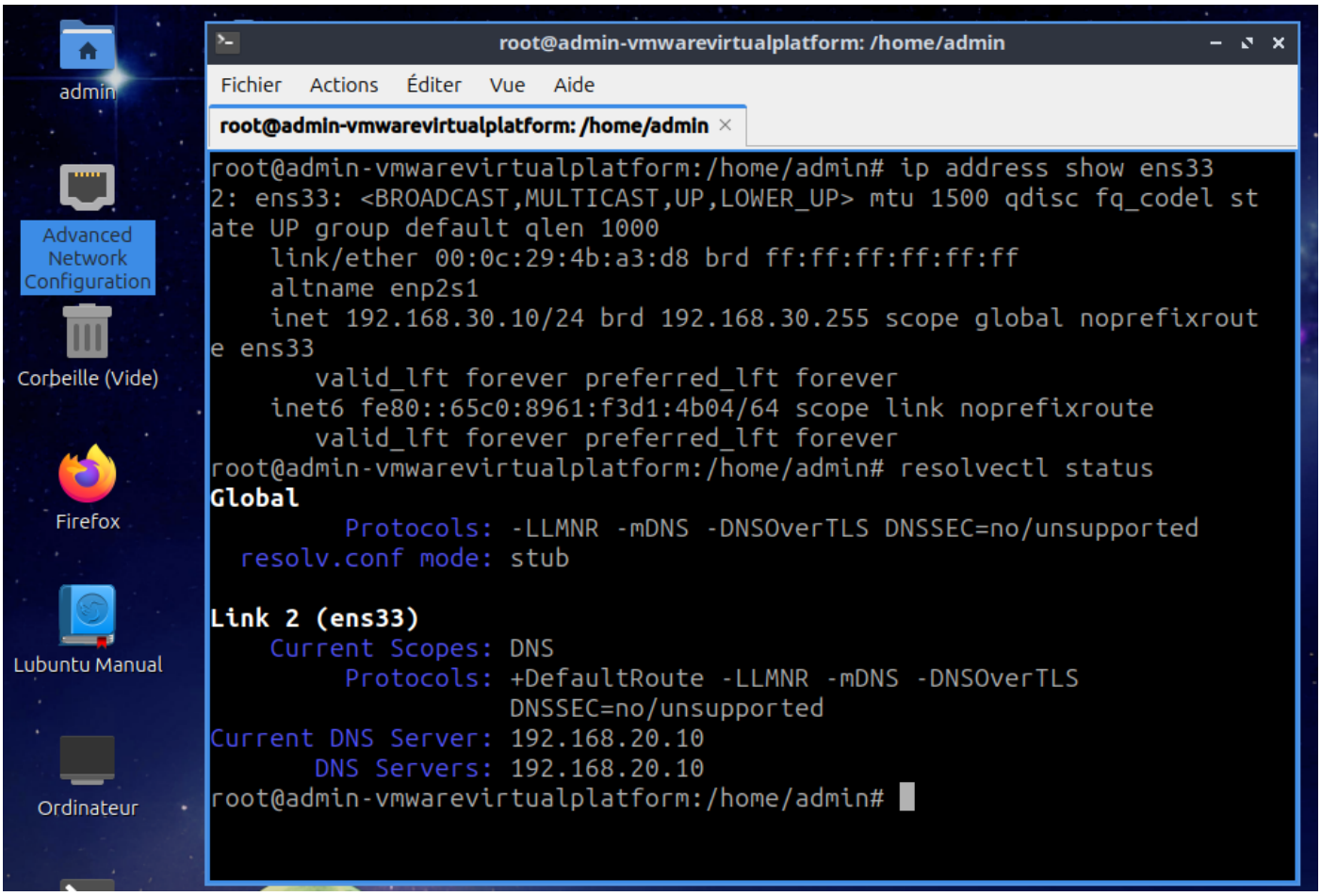


Image 4 : IP du serveur SFTP

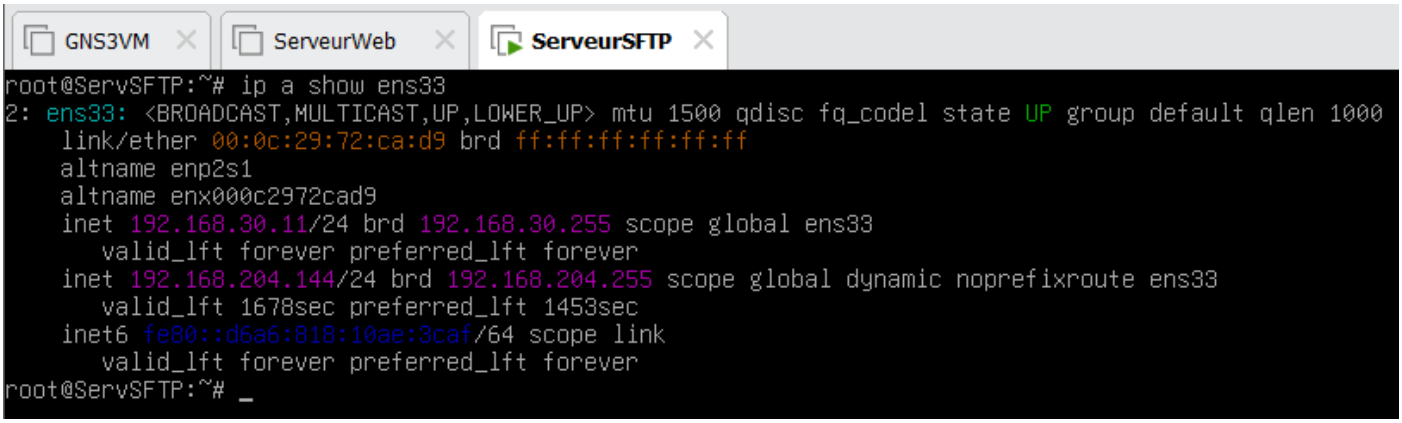
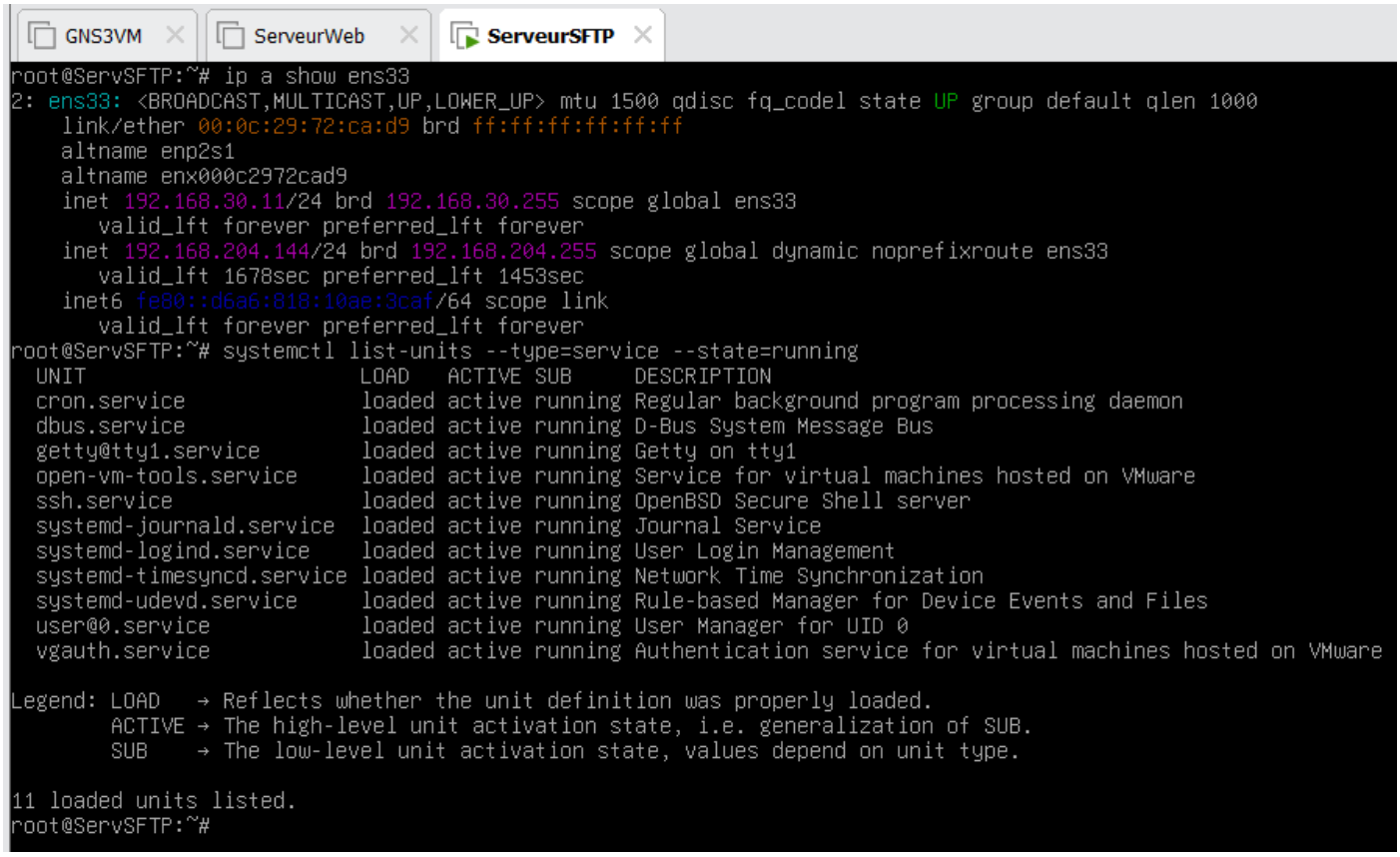


Image 5 : Service actif sur le serveur SFTP



Règles firewall pfSense

Des règles de filtrage ont été mises en place dans pfSense afin de contrôler les flux :

- Autorisation du trafic HTTP vers le serveur Web
- Autorisation du trafic SSH vers le serveur SFTP
- Autorisation requêtes DNS depuis DMZ vers le serveur Active Directory
- Interdiction d'accès direct de la DMZ vers le LAN

Ces règles garantissent l'isolation du réseau interne, permettent de limiter les accès uniquement aux services indispensables, renforçant ainsi la sécurité globale.

Dans ce projet, un alias de ports a été créé afin d'autoriser en une seule règle les flux nécessaires depuis la DMZ vers Internet (HTTP, HTTPS, DNS et NTP). Cela évite de multiplier les règles individuelles pour chaque port, ce qui rend la configuration plus lisible, plus facile à maintenir et moins sujette aux erreurs. En cas de modification (ajout ou suppression d'un port), il suffit de mettre à jour l'alias sans avoir à modifier toutes les règles associées.

Image 6 : Mise en place des aliases

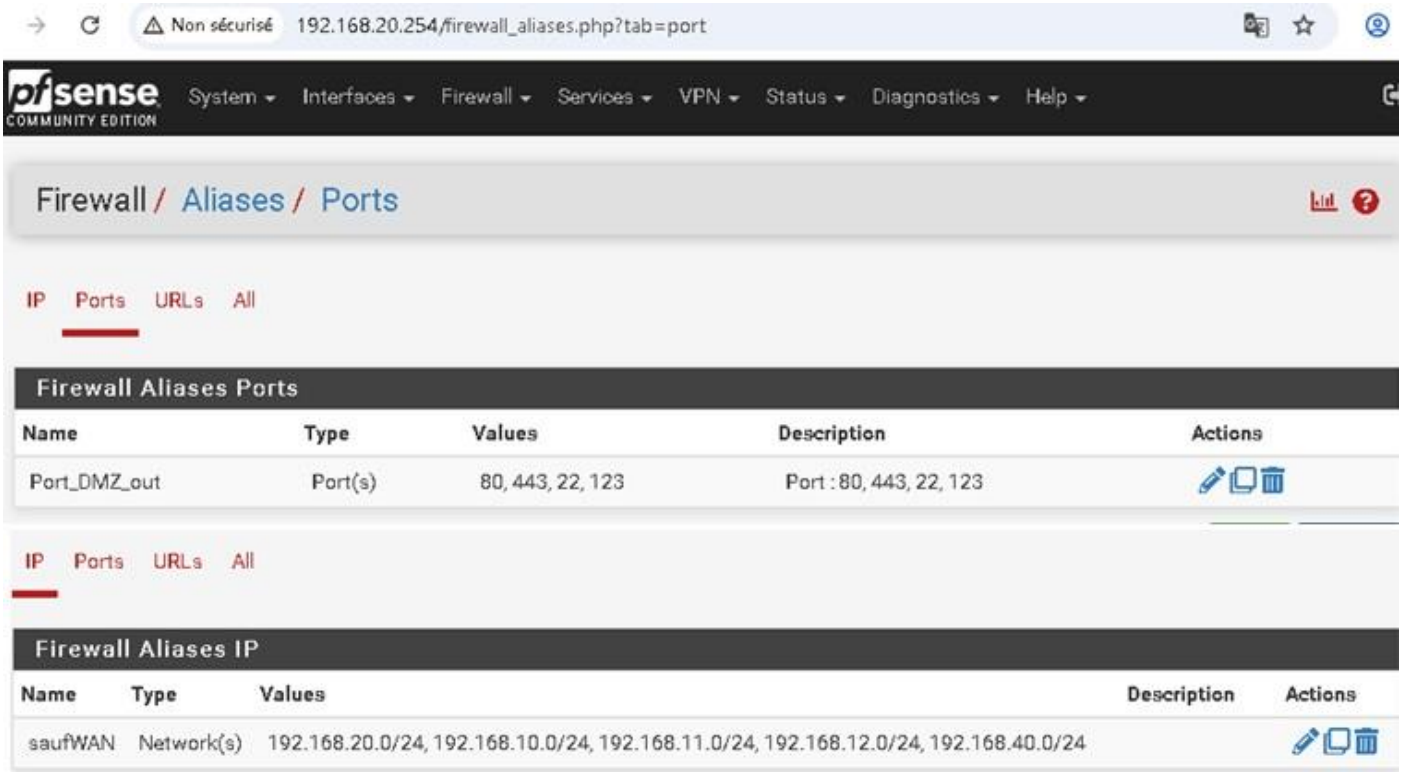
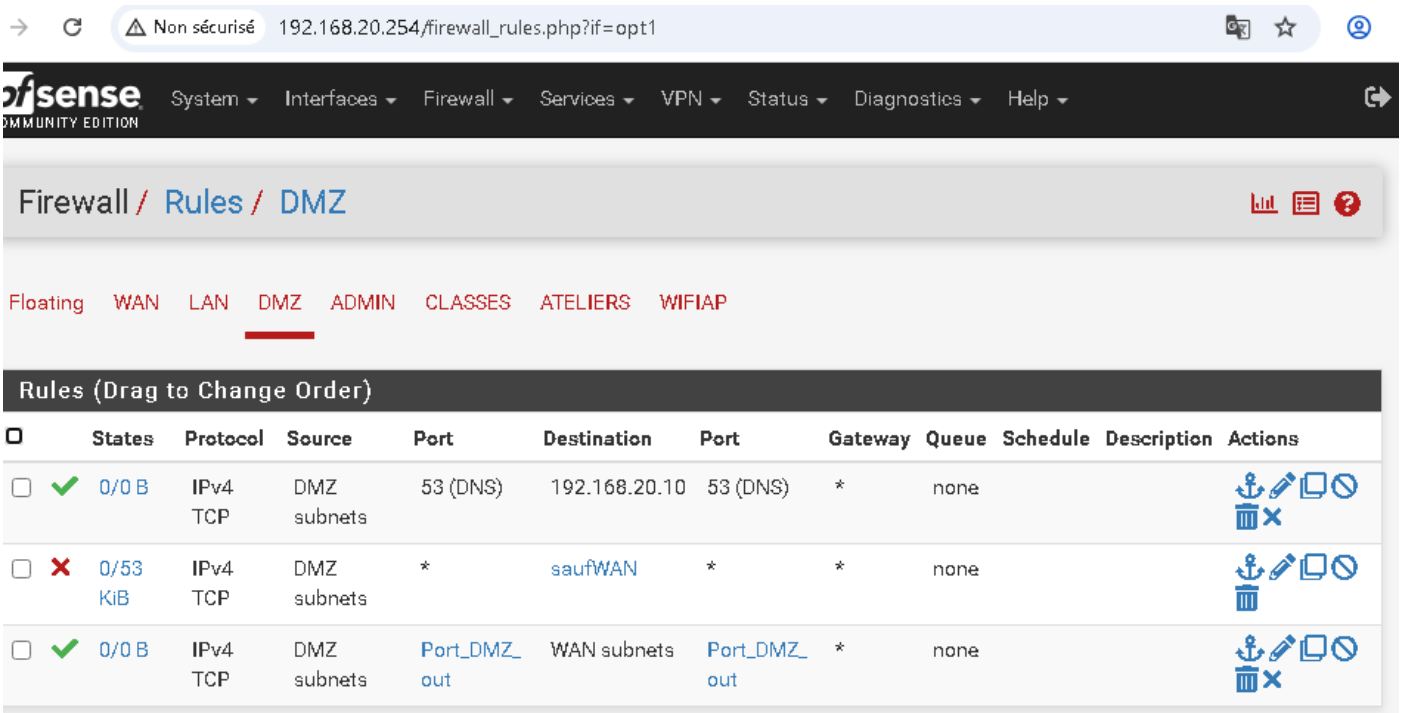


Image 7 : Règles DMZ en pfsense



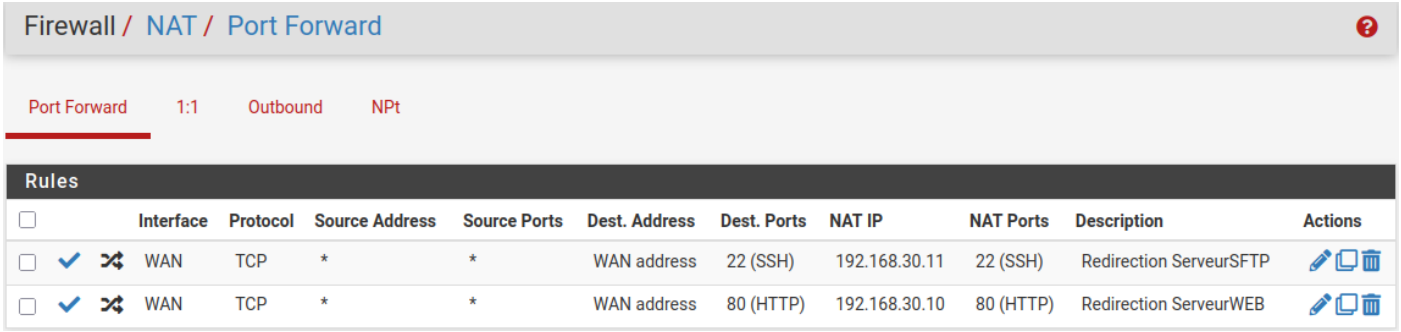
NAT

Une configuration NAT a été réalisée afin de rendre les services accessibles depuis Internet :

- Redirection du port 80 vers 192.168.30.10
- Redirection du port 21 vers 192.168.30.11

Cela permet aux utilisateurs externes d'accéder aux services sans exposer directement le réseau interne.

Image 8 : NAT Port Forward



Tests et validation

Plusieurs tests ont été réalisés :

- Accès au site Web depuis un poste client, Connexion SFTP fonctionnelle
- Blocage des accès vers le réseau interne

Les résultats montrent que la DMZ fonctionne correctement et sécurise l'infrastructure.

Image 9 : Accès site web depuis un client

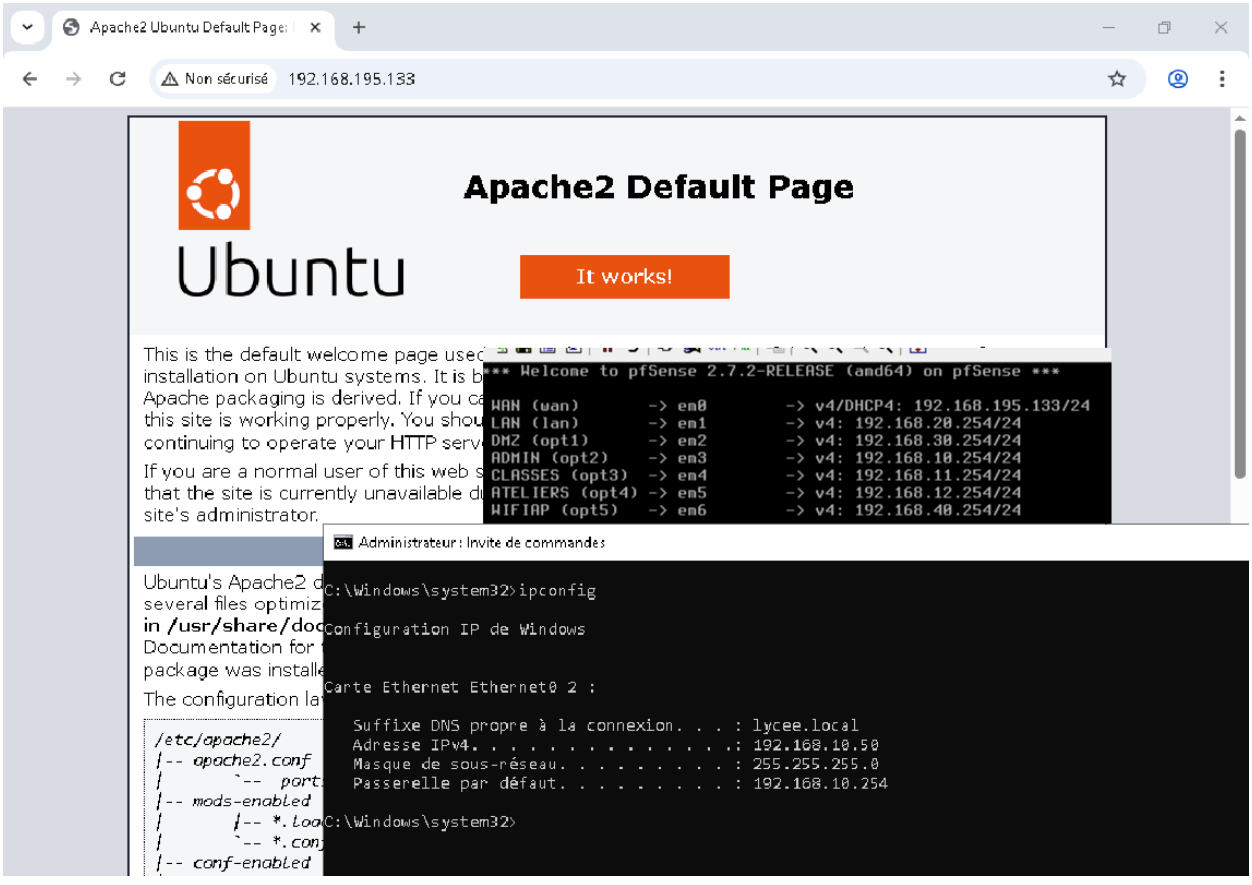


Image 11 : Ping / refus d'accès LAN

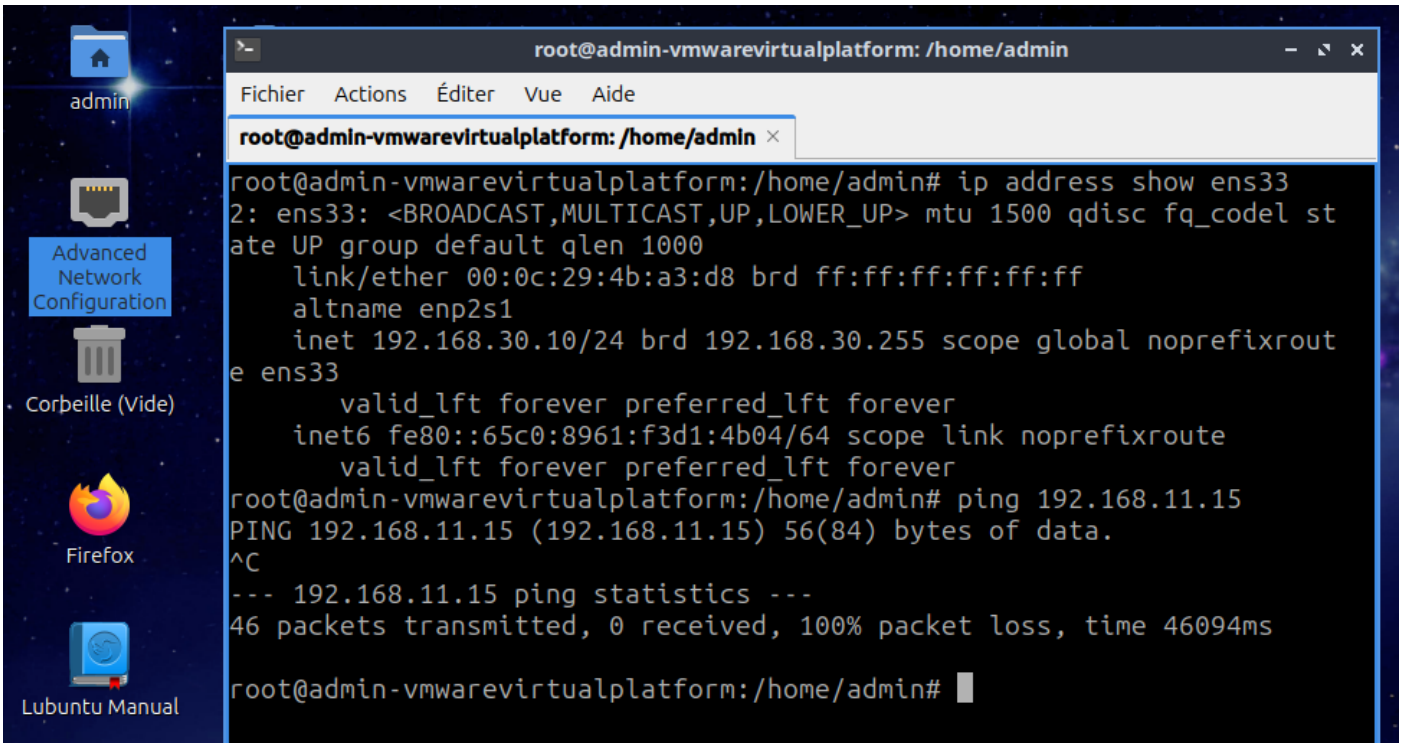
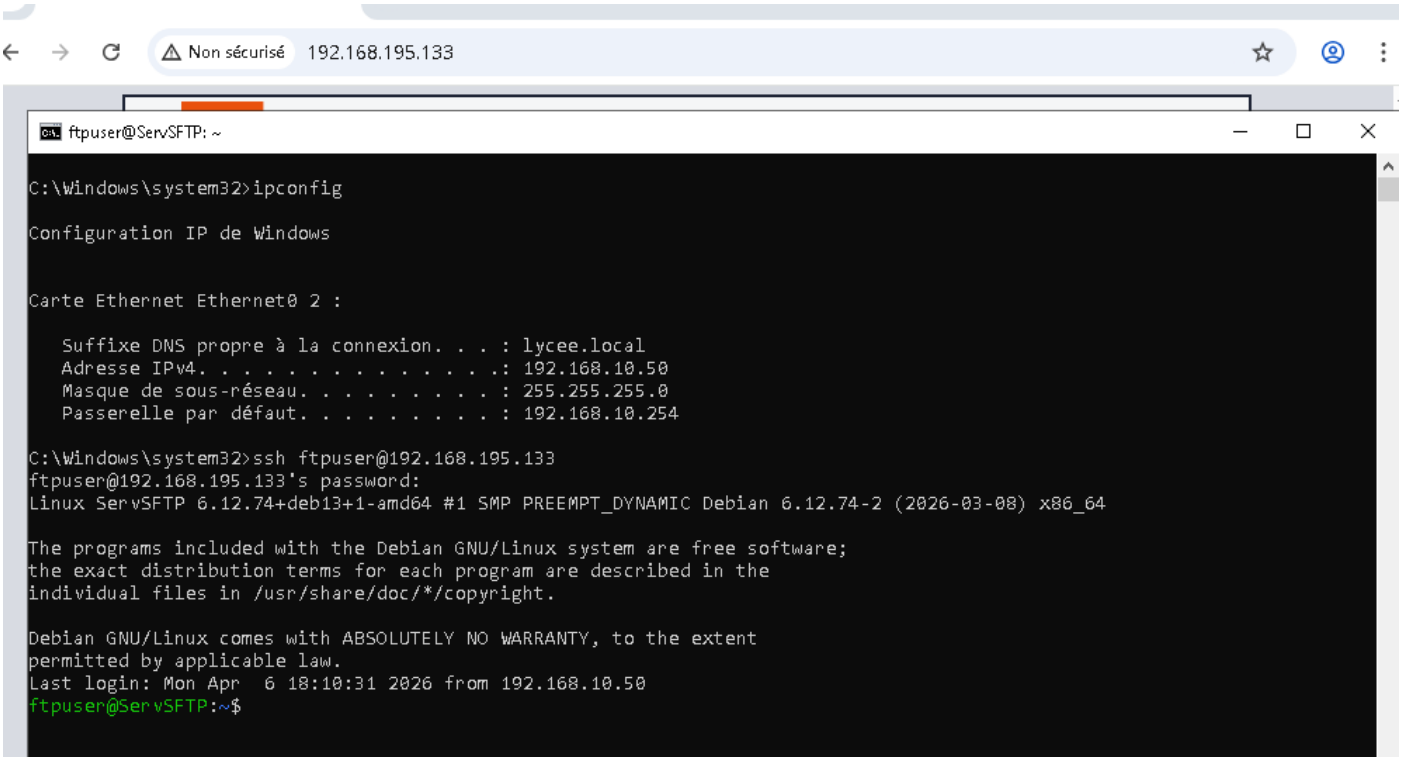


Image 12 : Connexion SFTP depuis poste client



Conclusion

Ce TP m'a permis de comprendre l'importance de la segmentation réseau et du rôle d'une DMZ dans la sécurisation d'une infrastructure.

La mise en place de pfSense et des règles associées m'a permis de maîtriser les notions de filtrage, NAT et gestion des flux.