



LE DMZ, MISE EN PLACE ET SECURISATION

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

MR MICHELE MASTROGIACOMO

Introduction	PAG. 1
Contexte et présentation de l'infrastructure	PAG. 2
• Image 1 : Schema segmentation réseau	
Objectifs de la DMZ	PAG. 3
Mise en place de la DMZ	PAG. 4
4.1 Création du réseau DMZ dans pfSense	
• Image 2 : Interfaces pfSense (avec DMZ)	
4.2 Configuration des serveurs (Web / FTP)	PAG. 4
• Image 3 : IP du serveur Web	PAG. 5
• Image 4 : IP du serveur FTP	
• Image 5 : Service actif sur le serveur SFTP	PAG. 6
4.3 Configuration des règles de pare-feu	
• Image 6 : Mise en place des alias	PAG. 7
• Image 7 : Règles DMZ en pfsense	
4.4 Configuration du NAT (accès depuis Internet)	PAG. 8
• Image 8 : NAT Port Forward	
Tests et validation	
• Image 9 : Accès site web depuis un client	
• Image 10 : Ping / refus d'accès LAN	PAG. 9
• Image 11 : Connexion SFTP	PAG. 9
Conclusion	PAG. 10

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.

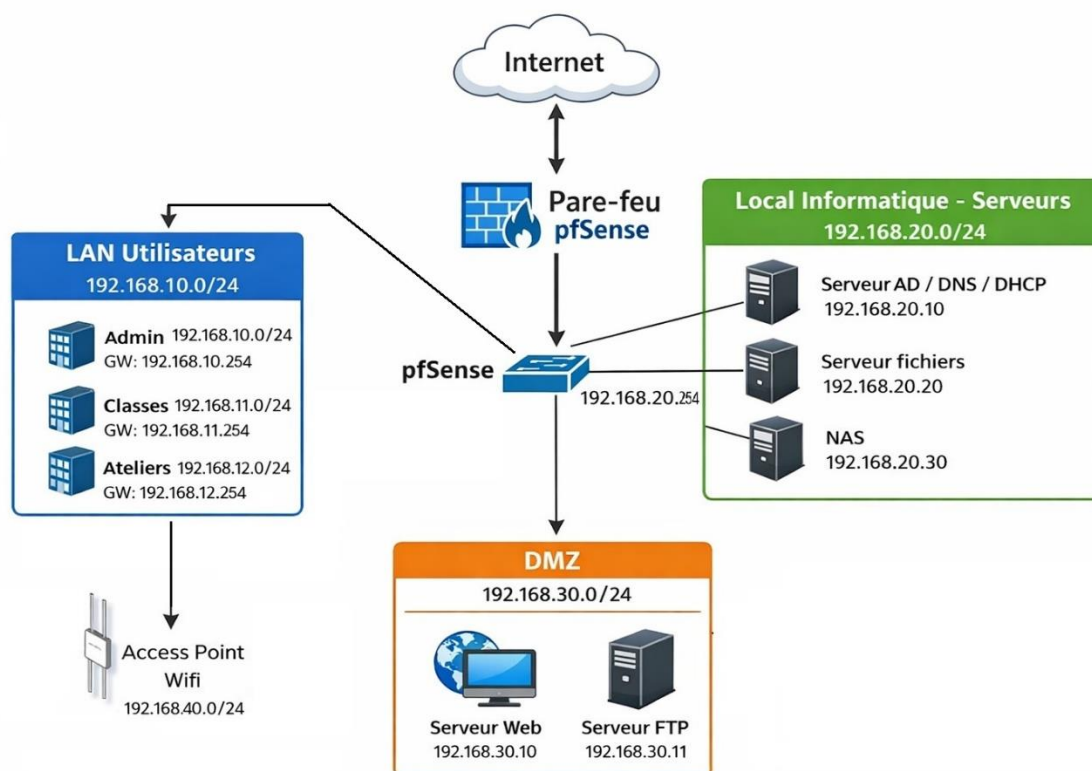
Contexte et présentation de l'infrastructure

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 où les données personnelles et la sécurité du système d'information doivent être optimales. Le contexte d'un périmètre scolaire et la présence d'utilisateurs ont 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 Ubuntu (192.168.30.10)
- un serveur SFTP avec Debian sans GUI (192.168.30.11)

Mise en place technique

Création de la DMZ dans pfSense

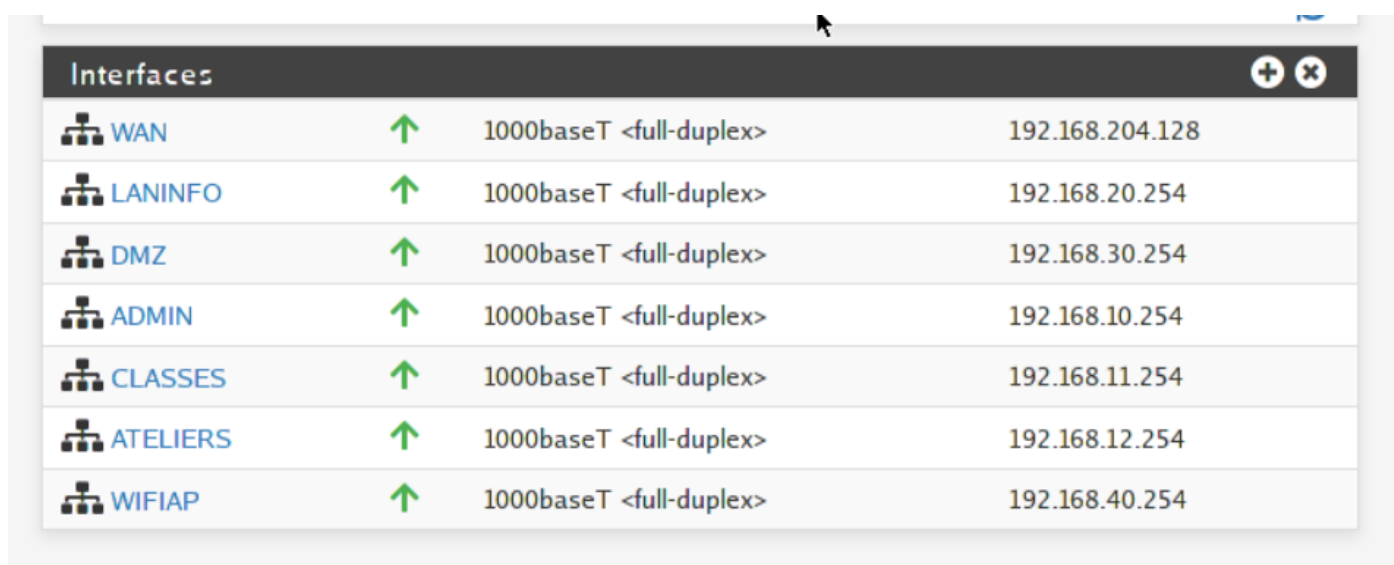
Comme première tâche une interface DMZ a été créée dans pfSense avec les paramètres suivants :

- 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)



Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.204.128
LANINFO	↑	1000baseT <full-duplex>	192.168.20.254
DMZ	↑	1000baseT <full-duplex>	192.168.30.254
ADMIN	↑	1000baseT <full-duplex>	192.168.10.254
CLASSES	↑	1000baseT <full-duplex>	192.168.11.254
ATELIERS	↑	1000baseT <full-duplex>	192.168.12.254
WIFIAP	↑	1000baseT <full-duplex>	192.168.40.254

Configuration des serveurs

Deux serveurs ont été déployés dans la DMZ :

Serveur Web sous Lubuntu :

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

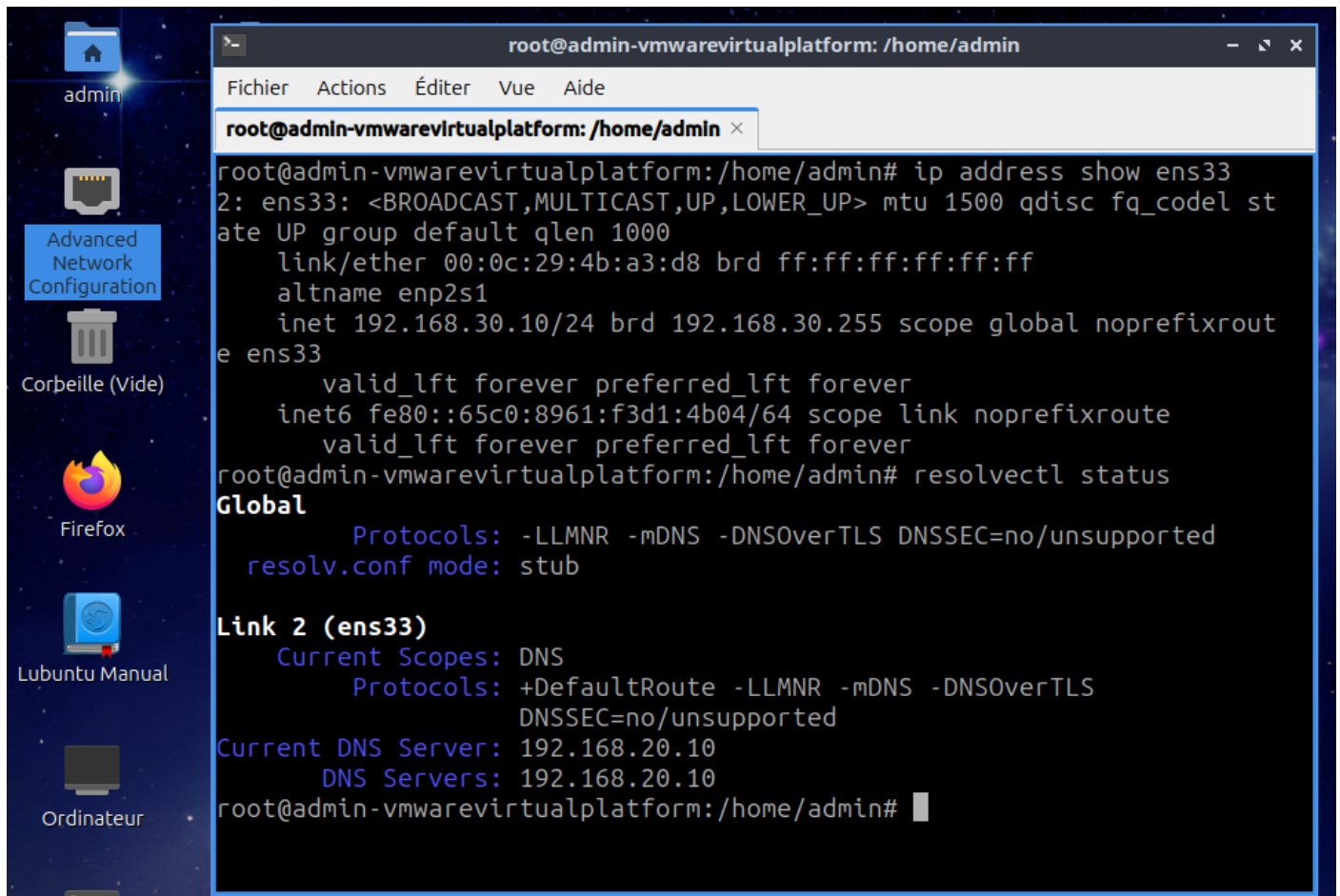
Serveur SFTP sous Debian sans GUI :

- 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)



The image shows a terminal window on a Linux desktop environment. The terminal prompt is root@admin-vmwarevirtualplatform: /home/admin. The user has executed the command 'ip address show ens33', which displays the following output:

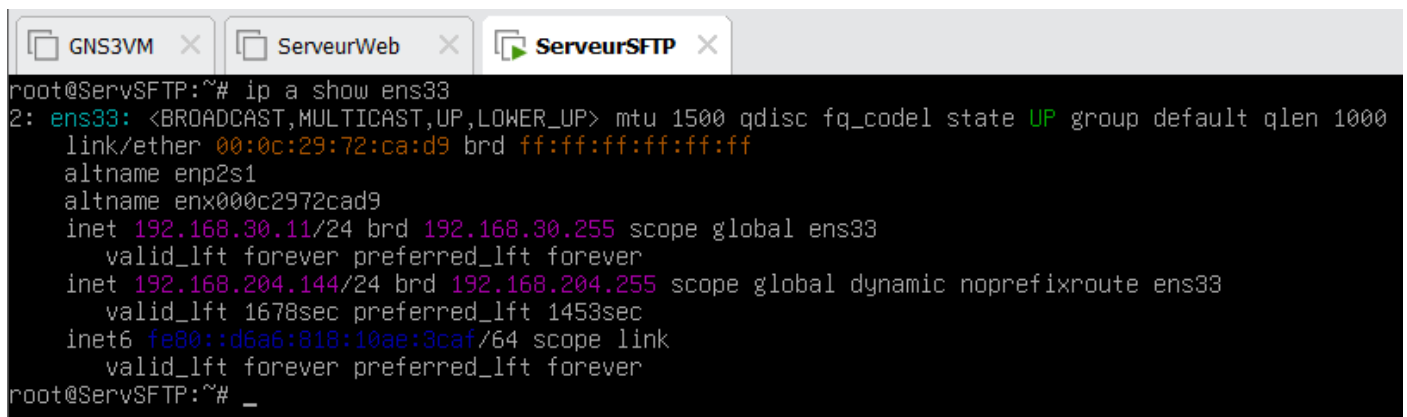
```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4b:a3:d8 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.30.10/24 brd 192.168.30.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::65c0:8961:f3d1:4b04/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Next, the user has executed 'resolvectl status', which shows the following output:

```
Global
    Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
    resolv.conf mode: stub

Link 2 (ens33)
    Current Scopes: DNS
    Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS
                DNSSEC=no/unsupported
    Current DNS Server: 192.168.20.10
    DNS Servers: 192.168.20.10
```

Image 4 : IP du serveur SFTP



The image shows a terminal window with three tabs: GNS3VM, ServeurWeb, and ServeursFTP. The active tab is ServeursFTP. The terminal prompt is root@ServSFTP:~#. The user has executed the command 'ip a show ens33', which displays the following output:

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:72:ca:d9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname enx000c2972cad9
    inet 192.168.30.11/24 brd 192.168.30.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.204.144/24 brd 192.168.204.255 scope global dynamic noprefixroute ens33
        valid_lft 1678sec preferred_lft 1453sec
    inet6 fe80::d6a6:818:10ae:3caf/64 scope link
        valid_lft forever preferred_lft forever
```

Image 5 : Service actif sur le serveur SFTP

```
GNS3VM x  ServerWeb x  ServeurSFTP x
root@ServSFTP:~# ip a show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:72:ca:d9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname enx000c2972cad9
    inet 192.168.30.11/24 brd 192.168.30.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.204.144/24 brd 192.168.204.255 scope global dynamic noprefixroute ens33
        valid_lft 1678sec preferred_lft 1453sec
    inet6 fe80::d6a6:818:10ae:3caf/64 scope link
        valid_lft forever preferred_lft forever
root@ServSFTP:~# systemctl list-units --type=service --state=running
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
cron.service                        loaded active running Regular background program processing daemon
dbus.service                        loaded active running D-Bus System Message Bus
getty@tty1.service                  loaded active running Getty on tty1
open-vm-tools.service               loaded active running Service for virtual machines hosted on VMware
ssh.service                         loaded active running OpenBSD Secure Shell server
systemd-journald.service            loaded active running Journal Service
systemd-logind.service              loaded active running User Login Management
systemd-timesyncd.service           loaded active running Network Time Synchronization
systemd-udev.service                loaded active running Rule-based Manager for Device Events and Files
user@.service                       loaded active running User Manager for UID 0
vgauth.service                      loaded active running Authentication service for virtual machines hosted on VMware

Legend: LOAD    → Reflects whether the unit definition was properly loaded.
         ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
         SUB    → The low-level unit activation state, values depend on unit type.

11 loaded units listed.
root@ServSFTP:~#
```

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

192.168.20.254/firewall_aliases.php?tab=port

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Aliases / Ports

IP Ports URLs All

Name	Type	Values	Description	Actions
Port_DMZ_out	Port(s)	80, 443, 22, 123	Port : 80, 443, 22, 123	

IP Ports URLs All

Name	Type	Values	Description	Actions
saufWAN	Network(s)	192.168.20.0/24, 192.168.10.0/24, 192.168.11.0/24, 192.168.12.0/24, 192.168.40.0/24		

Image 7 : Règles DMZ en pfSense

192.168.20.254/firewall_rules.php?if=opt1

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / DMZ

Floating WAN LAN DMZ ADMIN CLASSES ATELIERS WIFIAP

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	DMZ subnets	53 (DNS)	192.168.20.10	53 (DNS)	*	none			
<input type="checkbox"/> 0/53 KiB	IPv4 TCP	DMZ subnets	*	saufWAN	*	*	none			
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	DMZ subnets	Port_DMZ_out	WAN subnets	Port_DMZ_out	*	none			

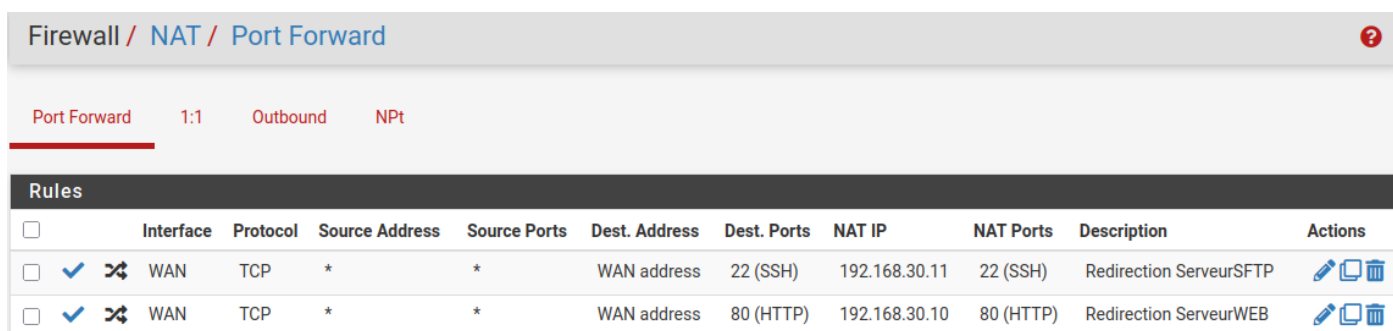
NAT

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



Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	22 (SSH)	192.168.30.11	22 (SSH)	Redirection ServeurSFTP	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.30.10	80 (HTTP)	Redirection ServeurWEB	

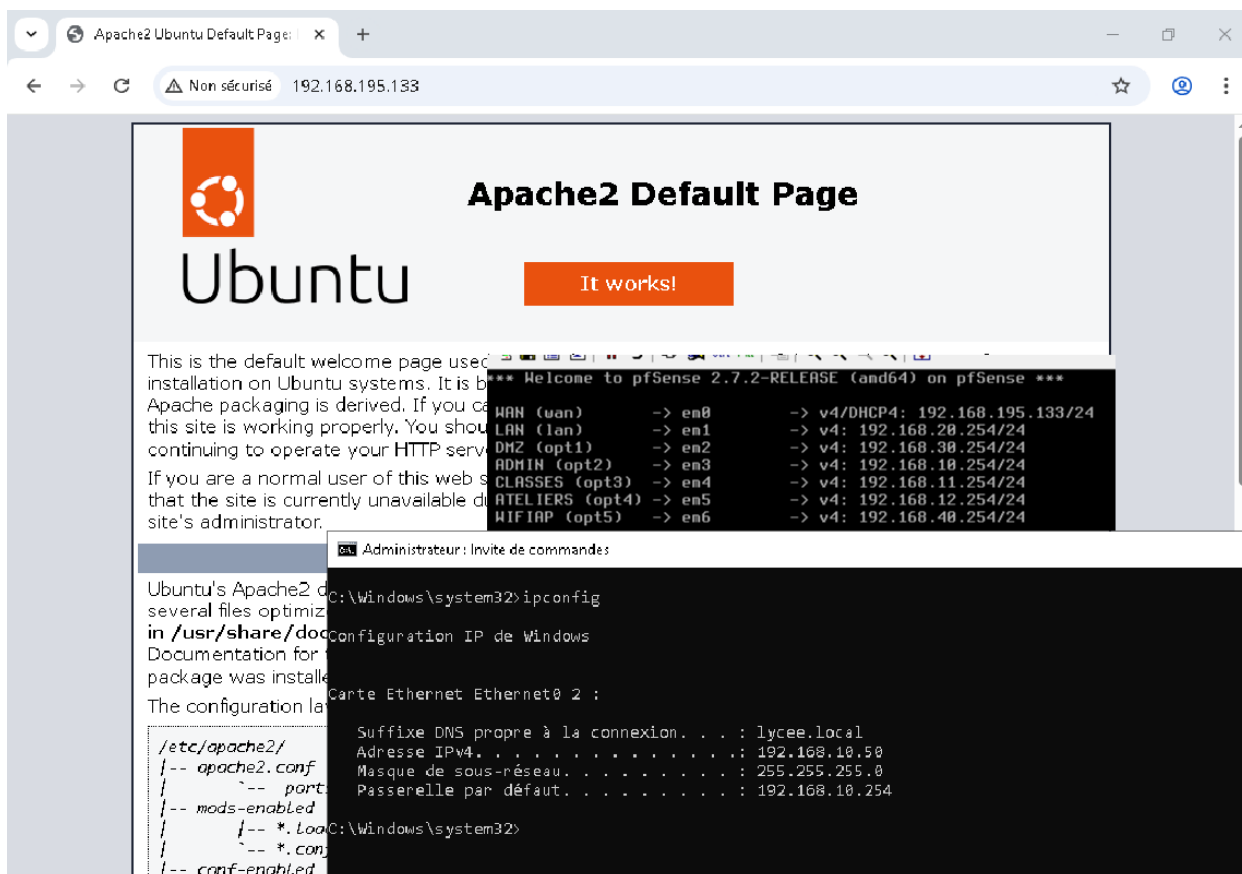
Tests et validation

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



Administrateur: Invite de commandes

```
C:\Windows\system32>ipconfig
Configuration IP de Windows
Carte Ethernet Ethernet0 2 :
    Suffixe DNS propre à la connexion. . . : lycee.local
    Adresse IPv4. . . . . : 192.168.10.50
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.10.254
C:\Windows\system32>
```

Image 11 : Ping / refus d'accès LAN

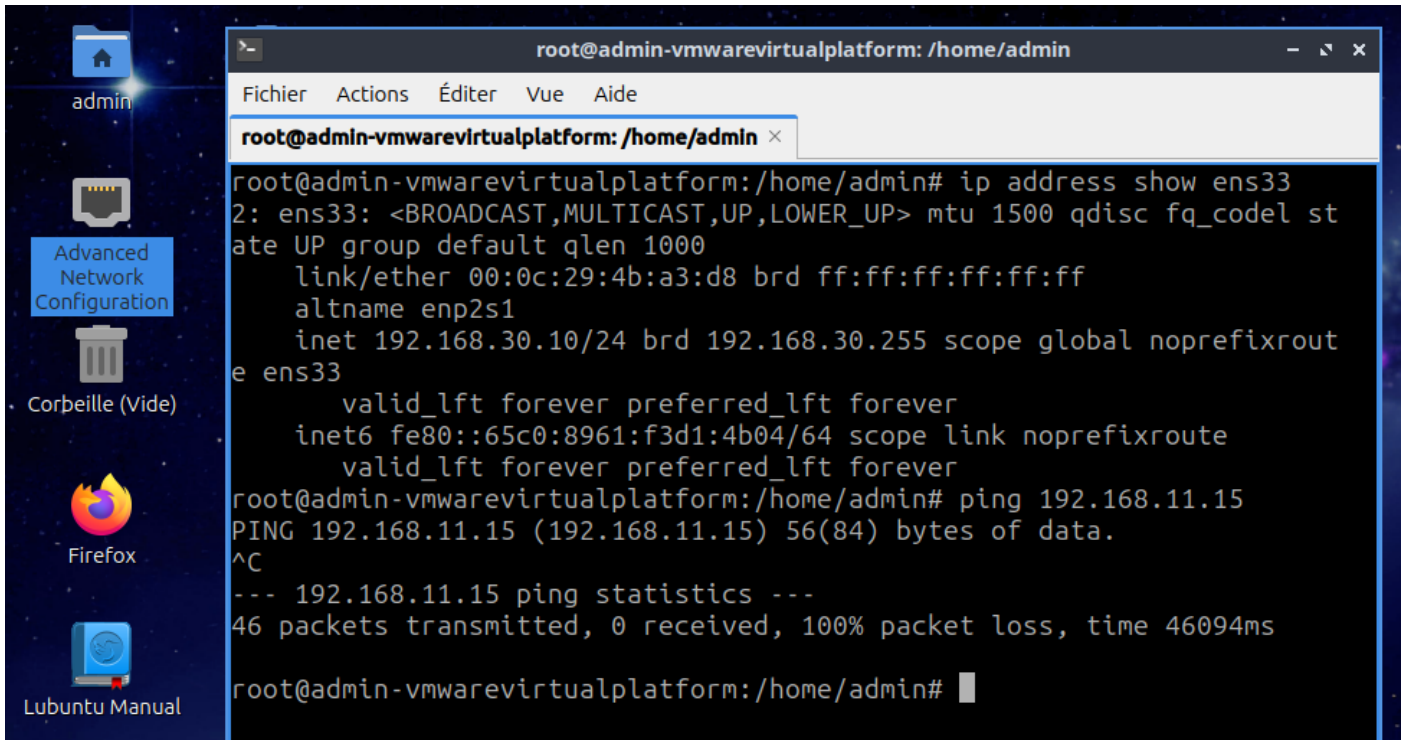
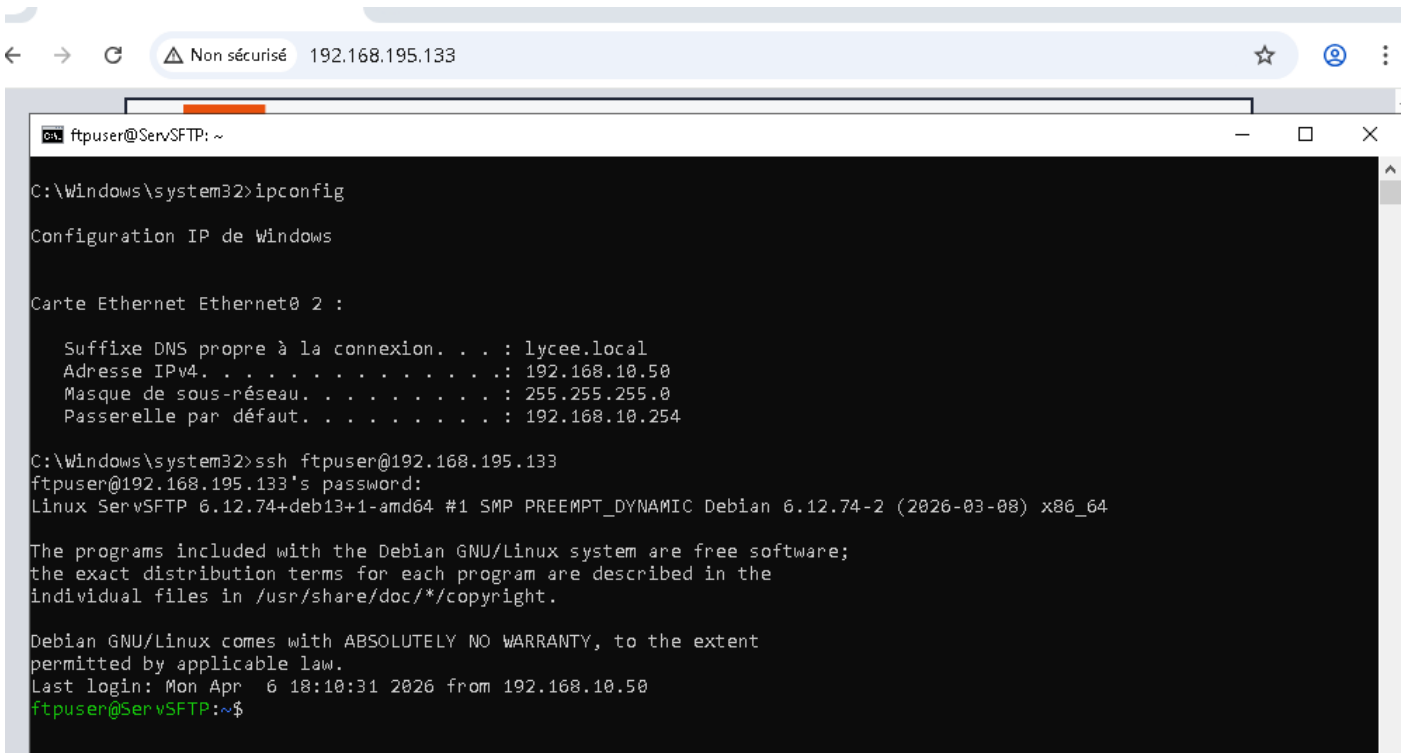


Image 12 : Connexion SFTP depuis poste client



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.