Rapport TSSR : Projet Lab VMware

Jean-Paul MELISSE

1 Introduction

Ce projet s'inscrit dans une démarche d'apprentissage autonome dans le domaine de l'administration des systèmes et des réseaux, suite à une formation TSSR (Technicien Systèmes et Réseaux) partiellement suivie. L'objectif est de concevoir et déployer un laboratoire réseau complet en environnement virtualisé à l'aide de VMware Workstation.

La PME fictive TechNova Solutions, spécialisée dans les services numériques, souhaite moderniser son infrastructure informatique. Ce projet simule la création d'un environnement réseau sécurisé, structuré et adapté aux besoins typiques d'une petite entreprise : gestion centralisée des utilisateurs, partage de ressources, sécurité réseau, et hébergement de services accessibles depuis l'extérieur.

Ce projet permet de mettre en pratique plusieurs compétences clés du métier de technicien systèmes et réseaux : installation de services réseau, sécurisation via un pare-feu (pfSense), configuration d'un domaine Active Directory, mise en place de GPO, et tests de connectivité.

2 Cahier des charges

2.1 Objectifs techniques

L'infrastructure mise en place devra permettre à l'entreprise de :

- Centraliser la gestion des comptes utilisateurs via un serveur Active Directory (AD).
- Partager des fichiers entre services grâce à un serveur de fichiers avec contrôle d'accès.
- Sécuriser l'infrastructure réseau grâce à un pare-feu (pfSense) avec une séparation logique des zones LAN / DMZ / WAN.
- Héberger un site web consultable depuis l'extérieur dans une zone isolée (DMZ).
- Tester les règles de sécurité réseau (isolation, filtrage, journalisation).

2.2 Contraintes

- L'ensemble du projet doit être réalisé en environnement virtualisé, avec VMware Workstation.
- L'infrastructure sera entièrement locale, sans perturber le réseau domestique existant.
- Les IP seront définies en adresses privées selon une topologie personnalisée.
- Aucun accès physique à du matériel réel (switchs, câblage) n'est requis.

2.3 Résultats attendus

- Fonctionnement opérationnel de tous les services déployés (AD, DNS, DHCP, partage de fichiers, serveur web).
- Tests concluants sur la connectivité réseau, la sécurité (firewall) et les GPO.
- Rapport complet structurant toutes les étapes du projet et justifiant les choix techniques.

3 Conception de l'infrastructure

3.1 Architecture réseau logique

L'infrastructure est segmentée en trois zones réseau distinctes simulant des VLANs virtuels via VMware Workstation :

- LAN (Réseau local) : regroupe les serveurs internes (AD, fichiers) et les postes clients.
- DMZ (Zone démilitarisée) : contient le serveur web accessible depuis l'extérieur.
- WAN (réseau externe simulé) : représente Internet et les machines externes.

Chaque zone est isolée sur une interface dédiée du pare-feu pfSense, qui gère le routage interzones et applique les règles de sécurité.

Zone	Nom du réseau VMware	Adresse IP	Rôle
WAN	VMnet1	192.168.10.0/24	Accès externe (Internet simulé)
LAN	VMnet2	192.168.100.0/24	Réseau interne sécurisé
DMZ	VMnet3	192.168.200.0/24	Zone semi-ouverte (serveur web)

Table 1: Architecture réseau logique simulée sous VMware

3.2 Plan d'adressage IP

Machine	Système d'exploitation	Adresse IP	Réseau
pfSense (WAN)	pfSense	192.168.10.1	VMnet1
pfSense (LAN)	pfSense	192.168.100.1	VMnet2
pfSense (DMZ)	pfSense	192.168.200.1	VMnet3
Serveur AD/DNS/DHCP	Windows Server 2022	192.168.100.10	LAN
Serveur de fichiers	Windows Server 2022	192.168.100.11	LAN
Client Admin	Windows 10 Pro	192.168.100.100 (DHCP)	LAN
Client Direction	Windows 10 Pro	192.168.100.101 (DHCP)	LAN
Serveur Web	Debian 12 / Ubuntu	192.168.200.10	DMZ
Machine Externe (test)	Windows / Linux	192.168.10.50	WAN

Table 2: Plan d'adressage IP

3.3 Schéma réseau et Simulation avec Cisco Packet Tracer

Dans le cadre du projet, une version simulée de l'architecture réseau a été réalisée avec Cisco Packet Tracer. Bien que Packet Tracer ne permette pas de simuler directement des appliances comme pfSense

ou VMware, une modélisation équivalente a été construite pour visualiser les flux réseau, tester les règles de routage et configurer des éléments de base (ex : routeurs, VLAN, serveurs).

La Figure 1 illustre la topologie de l'infrastructure à travers un schéma réseau réalisé dans Cisco Packet Tracer.

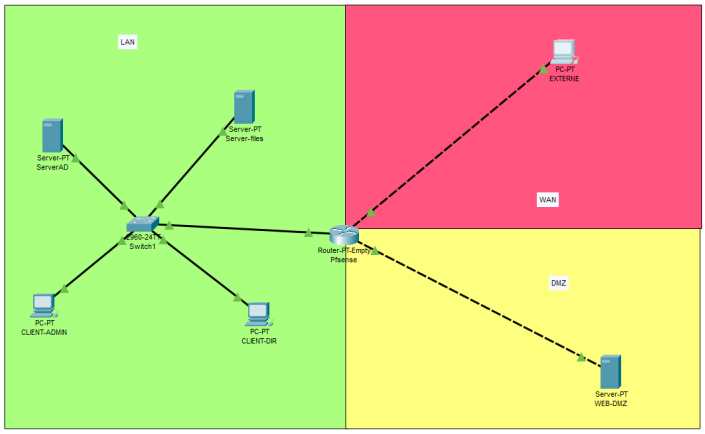

Figure 1: Schéma de l'infrastructure sur Cisco Packet Tracer

Fichier de simulation : Le fichier `cisco_lab_tssr.pkt` est disponible dans le dépôt GitHub du projet sous `/configs/`.

Configuration du routeur simulant pfSense Sur le "pfSense" simulé avec un routeur Cisco, on configure :

- Les trois interfaces correspondant aux zones LAN, DMZ et WAN.
- Le protocole RIP (ou du routage statique) pour l'interconnexion des zones.
- Des règles ACL pour sécuriser l'accès réseau.

La configuration se fait depuis le terminal CLI :

- "enable" pour passer en mode privilégié
- "configure terminal" pour entrer en mode de configuration

Mise en place des règles ACL :

- Pour commencer, on veut que seul le serveur web est accessible depuis l'extérieur (uniquement l'accès HTTP - port 80). Donc on tape la ligne :

```
access-list 100 permit tcp any host 192.168.200.10 eq 80
```

- Puis, on refuse tout autre accès aux autres services du serveur depuis l'extérieur. On tape la commande :

```
access-list 100 deny ip any 192.168.200.0 0.0.0.255
```

- On fait de même avec le LAN. On coupe tout accès depuis l'extérieur. On tape :

```
access-list 100 deny ip any 192.168.100.0 0.0.0.255
```

- Enfin, on autorise les connexions sortantes. On tape :

```
access-list 100 permit ip any any
```

On va aussi ajouter une redirection vers le serveur web depuis le routeur côté extérieur (WAN) sur le port 80 (accès http). On tape la commande : "ip nat inside source static tcp 192.168.200.10 80 192.168.10.1 80". Pour que cette ligne fonctionne, il faut déclarer les accès inside et outside de la table nat. On modifie l'interface côté DMZ "ici en tapant interface g7/0" et on tape la commande "ip nat inside" pour l'indiquer à la table nat. On tape "exit" pour sortir de l'interface DMZ. On fait de même du côté WAN "ici en tapant interface g9/0" et on tape la commande "ip nat outside" pour l'indiquer à la table nat. Enfin, l'ACL (qui sont des règles ACL étendues) est appliquée sur l'interface WAN en entrée. On tape donc la ligne : "ip access-group 100 in". On peut voir les étapes précédentes sur la Figure 2.

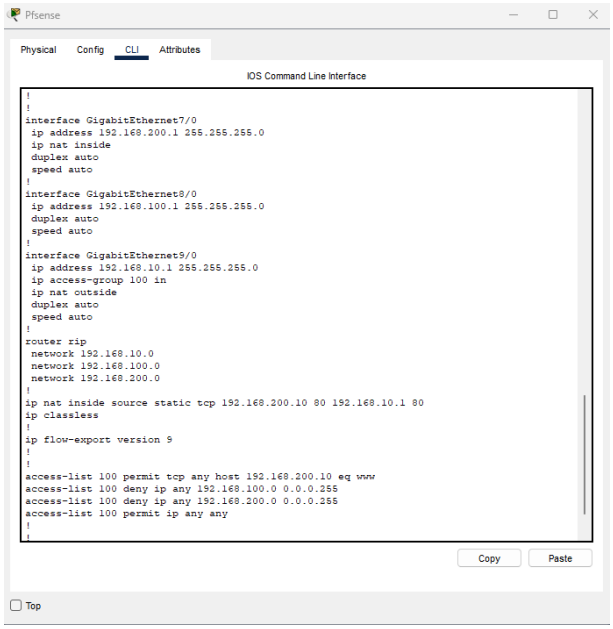

Figure 2: Configuration de Pfsense dans Packet Tracer

Configuration des services internes On va aussi configurer les autres machines et surtout le serveur Active Directory. Ce dernier est configuré pour jouer également le rôle de serveur DHCP pour les clients du LAN (Voir la Figure 3).

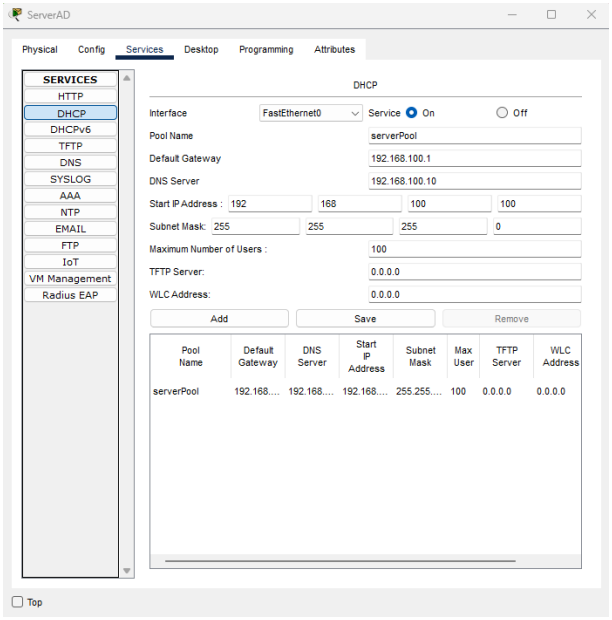

Figure 3: Configuration du service DHCP dans Packet Tracer

Tests de connectivité entre zones

Sur la machine externe, on essaie de se connecter au DMZ et au LAN avec la commande `ping`. On voit sur la Figure 4 qu'on n'y arrive pas.

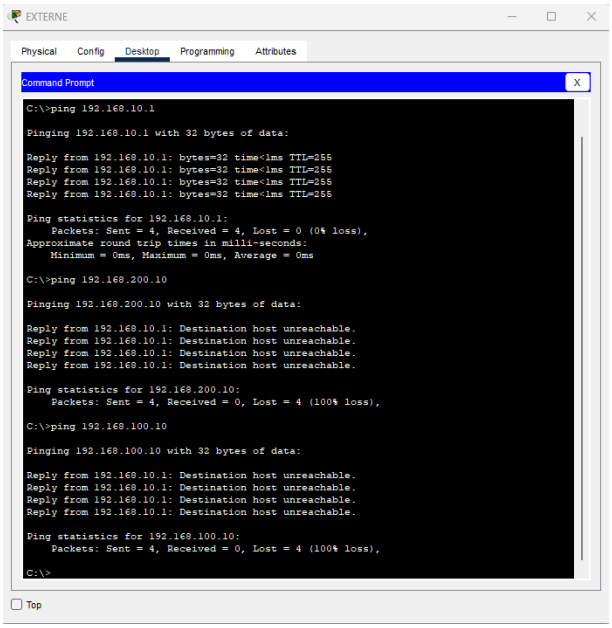

Figure 4: Blocage des pings vers les zones internes

Par contre, sur la machine externe, on voit qu'on arrive à accéder à la page web du serveur sur la DMZ grâce à la redirection (Voir la Figure 5).

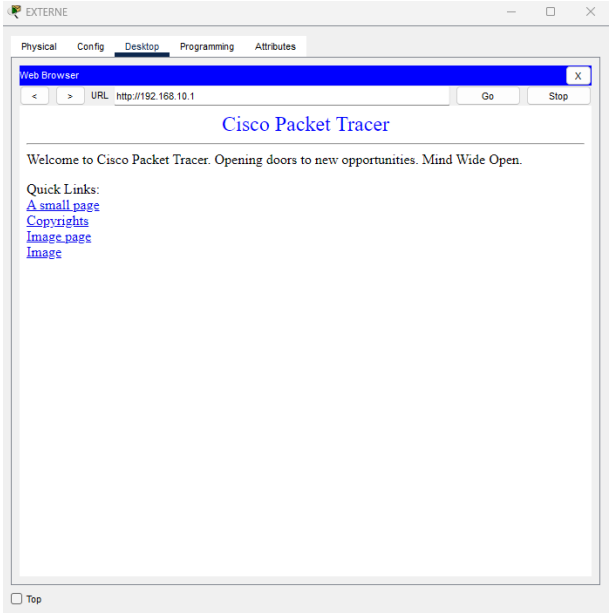

Figure 5: Accès au site Web de la DMZ depuis l'extérieur

Concernant la connexion entre les machines LAN et le serveur en DMZ, on peut voir sur les Figures 6 et 7 que la communication entre les machines se passe sans problème.

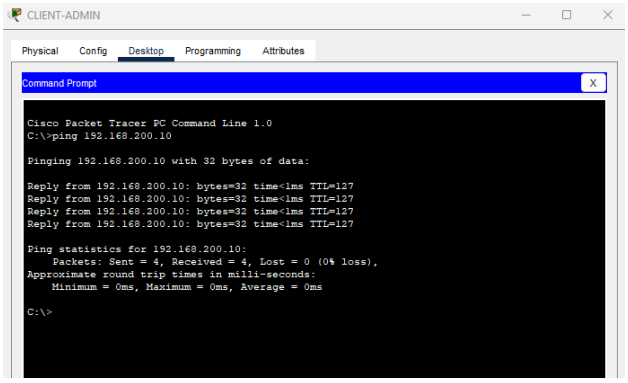

Figure 6: Connexion entre le LAN et le DMZ - coté LAN

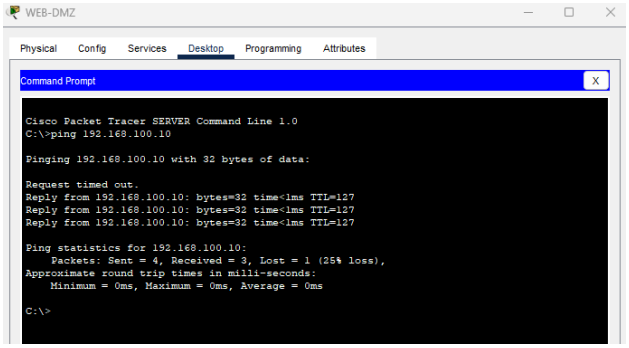

Figure 7: Connexion entre le LAN et le DMZ - coté DMZ

3.3.1 Renforcement de la sécurité sur l'interface WAN

Afin de limiter les informations divulguées à l'extérieur, certaines options ont été désactivées sur l'interface WAN du routeur simulant pfSense. Cela permet de réduire la surface d'attaque et de ne pas répondre inutilement à des requêtes réseau potentiellement malveillantes.
Voici les commandes appliquées sur l'interface WAN (g9/0) :

- no ip icmp unreachable ! Ne répond pas aux paquets bloqués (ACL) [non supporté dans Packet Tracer]
- no ip redirects ! Empêche l'envoi de redirections ICMP [non supporté dans Packet Tracer]
- no ip proxy-arp ! Empêche le proxy ARP (évite certaines attaques réseau)

Ces paramètres rendent le comportement du pare-feu plus silencieux :

- Un paquet bloqué par une règle ACL n'est pas suivi d'un message "ICMP unreachable".
- Le routeur n'envoie pas de redirections de route qui pourraient être exploitées.
- Il ne répond pas à des requêtes ARP pour d'autres machines, ce qui réduit les risques d'empoisonnement ARP.

Dans Cisco Packet Tracer, seule la commande no ip proxy-arp est fonctionnelle. Les deux autres commandes sont des bonnes pratiques de sécurité qu'on retrouve dans des environnements Cisco réels, mais qui ne sont pas implémentées dans ce simulateur.