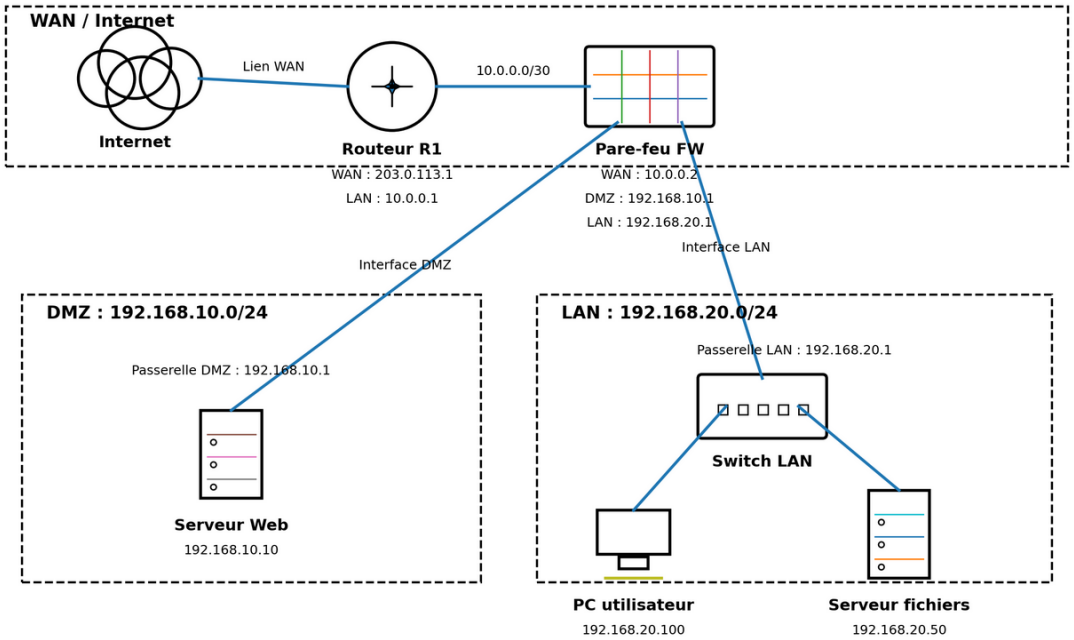
TD 1
Les réseaux

Contexte

Une entreprise possède 3 zones réseau :



@IP R1 côté Internet (WAN) : 203.0.113.1
Interface du pare-feu : WAN, DMZ et LAN

Partie 1 – Compréhension du réseau

1. Identifier les trois zones du réseau.
   - Internet
   - DMZ
   - LAN interne

2. Quel est le rôle de la DMZ ?
   La DMZ permet d'isoler le serveur WEB accessible depuis Internet par rapport au LAN. 1.
   Si le serveur WEB était dans le LAN, une attaque du serveur Web donnerai directement accès au réseau interne.

3. Quel équipement protège le LAN ?
   C'est le pare-feu.

4. Citer un actif critique de l'entreprise.
   On a : les données, serveur fichiers, serveur Web, postes utilisateurs.

Partie 2 – Table de routage

Compléter la table de routage du pare-feu :

Destination	Masque	Passerelle	Interface sortie
192.168.10.0	255.255.255.	Accès direct	DMZ
192.168.20.0	255.255.255.0	Accès direct	LAN
(Route par défaut) 0.0.0.0	0.0.0.0	10.0.0.1	WAN

Partie 3 – Règles de sécurité

Proposer des règles de sécurité pour :

- Depuis internet, je dois pouvoir accéder au serveur WEB mais pas au LAN.
- Depuis le LAN, je dois pouvoir accéder à Internet et au serveur WEB.
- Depuis la DMZ je ne dois pas accéder au LAN.

Source	Destination	Service	Action
Internet	Serveur WEB	HTTPS	Autoriser
Internet	LAN	Tous les services	Refuser
LAN	Internet	HTTP / HTTPS	Autoriser
DMZ	LAN	Tous les services	Refuser
LAN	Serveur WEB	HTTPS	Autoriser

Pour vous aidez à compléter le tableau :

- Source : Internet – DMZ - LAN
- Destination : Internet – DMZ – LAN – Serveur WEB
- Service : http – HTTPS – FTP – SMTP – POP – IMAP – Tous les services
- Action : Autoriser - Refuser

Partie 4 – Incident de cybersécurité

Un attaquant exploite une faille sur le serveur Web en DMZ.

1. Quelle zone est compromise en premier ?
   La DMZ

2. Pourquoi le LAN n'est-il pas forcément compromis immédiatement ?
   Parce que le pare-feu bloque les flux DMZ vers LAN.

3. Citer deux actions à réaliser après détection de l'incident.
   Exemples : isoler le serveur, analyser les logs, corriger la faille, changer les mots de passe, restaurer une sauvegarde saine.

1. Citer deux mesures préventives pour éviter ce type d'attaque.
   Exemples : mises à jour pare-feu, surveillance des logs, IDS/IPS, mots de passe forts, sauvegardes, limitation des accès.