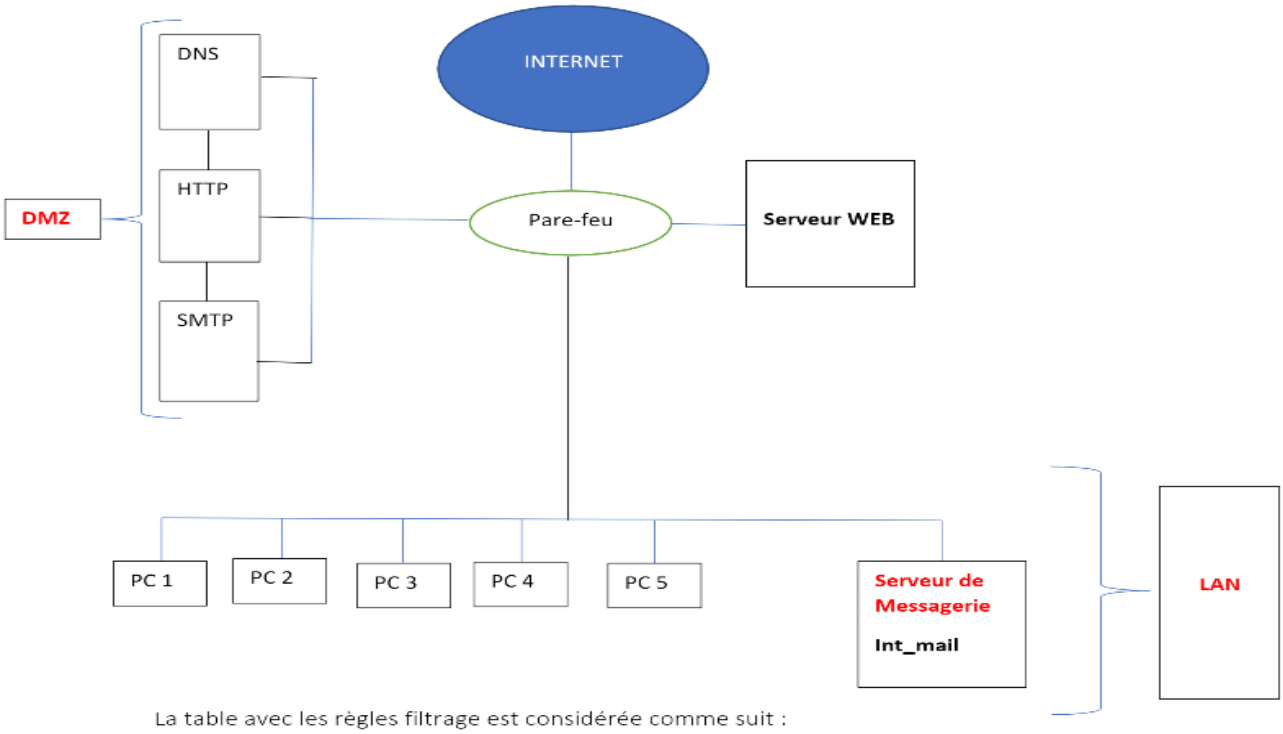
Exercice

On considère le réseau d'entreprise présenté dans la figure ci-dessous :



La table avec les règles filtrage est considérée comme suit :

N°	Source		Destination			Action
	Adresse	Port	Adresse	Port	Protocole	
1	Any	Any	DMZ_Web	HTTP	TCP	Drop
2	LAN	Any	DMZ_http	HTTP	TCP	Pass
3	LAN	Any	DMZ_Dns	DNS	UDP	Pass
4	Int_mail	Any	DMZ_smtp	SMTP	TCP	Drop
5	DMZ_SMTP	Any	Int_mail	SMTP	TCP	Pass
6	DMZ_HTTP	Any	Any	HTTP	TCP	Pass
7	DMZ_DNS	Any	Any	DNS	UDP	Drop
8	Any	Any	Any	Any	Any	Any

1 Tout trafic allant vers la DMZ Web via le port 80 est interdit

Donc : Obligation d'utiliser HTTPS

2 Tout trafic venant du LAN vers la DMZ_HTTP est autorisé

Réseau Local, donc pas de menace : HTTP autorisé

3 Les paquets venant du LAN vers le serveur DNS sont autorisés

Réseau Local, donc pas de menace : DNS autorisé

4 Aucun trafic venant du serveur de messagerie vers le serveur DMZ SMTP n'est autorisé

Les mails des employés doivent rester dans le serveur mail du réseau local

5 Le trafic venant du DMZ_SMTP vers le serveur de messagerie (interne) est autorisé

Le serveur mail de la DMZ peut joindre le serveur mail interne

6 Toutes les requêtes venant de la DMZ_HTTP sont autorisées à utiliser le port 80

La DMZ est sûre, elle n'est pas obligée d'utiliser le HTTPS, et peut utiliser le HTTP

7 Aucune requête venant de la DMZ_DNS n'est autorisée

Personne d'extérieure ne doit connaître les adresses IP du réseau local

8 Tout le reste est autorisé

Indispensable, sinon tout le reste serait interdit