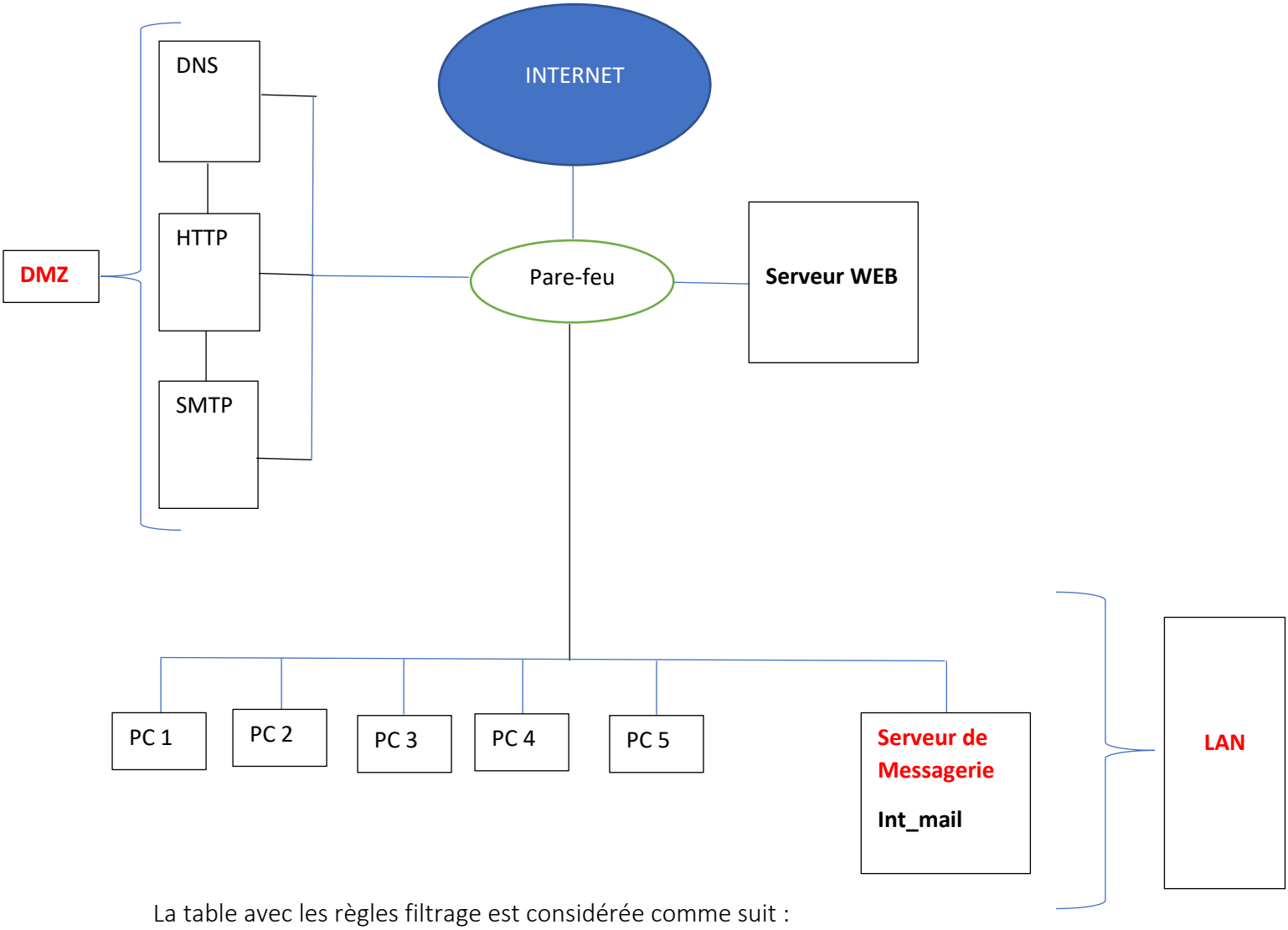
Exercice

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

Commentez la table de filtrage

Exercice Compréhension règles

```
!http://www.cnrs.fr/aquitaine-limousin/Delegation/STI/Cours/ACL
   -Cisco/ex-config-v11.html

version 11.0
no service config
no service tcp-small-servers
no service udp-small-servers
service password-encryption
!
logging 192.9.200.1
logging facility auth
!
hostname nom_du_cisco
!
enable password 7 XXXXXXXXXXXXXXXXXXX
!
! [..]
!
! Les access-lists
!
! Je vide les access-list courantes
no access-list 101
! Je n'accepte␣aucun␣paquet␣sur␣l'interface reseau du campus
   qui a comme
! adresse source une adresse dans mon reseau ou dans le reseau
! 127.0.0.0 (loopback)
access-list 101 deny ip 192.9.200.0 0.0.0.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
! Interdiction de ICMP (ping) sur l'adresse␣broadcast
access-list␣101␣deny␣icmp␣any␣host␣192.9.200.255␣log
access-list␣101␣deny␣icmp␣any␣host␣192.9.200.0␣log
!␣J'autorise ICMP sur toutes mes machines
access-list 101 permit icmp any 192.9.200.0 0.0.0.255
! Autorise le port 113 (RFC 931) sur mon serveur
```

```
access-list 101 permit tcp any host 192.9.200.1 eq 113
! Acces aux serveurs de noms primaires et secondaires
access-list 101 permit udp any host 192.9.200.1 eq domain
access-list 101 permit udp any host 192.9.200.2 eq domain
access-list 101 permit tcp any host 192.9.200.1 eq domain
access-list 101 permit tcp any host 192.9.200.2 eq domain
! Acces aux services usuels :
! NTP
access-list 101 permit udp any host 192.9.200.1 eq ntp
! TALK
access-list 101 permit udp any 192.9.200.0 0.0.0.255 eq 517
! FTP connexion de controle et de donnees
access-list 101 permit tcp any host 192.9.200.1 eq ftp
access-list 101 permit tcp any host 192.9.200.1 eq ftp-data
! Telnet
access-list 101 permit tcp any host 192.9.200.1 eq telnet
! SMTP
access-list 101 permit tcp any host 192.9.200.1 eq smtp
! WWW
access-list 101 permit tcp any host 192.9.200.1 eq www
! NNTP
access-list 101 permit tcp any host 192.9.200.210 eq nntp
! Autorise tous les ports TCP superieurs a 1024, a cause de FTP
    et TALK
access-list 101 permit tcp any 192.9.200.0 0.0.0.255 gt 1023
! Autorise tous les ports UDP superieurs a 1024 sauf 2049 (NFS)
access-list 101 deny udp any 192.9.200.0 0.0.0.255 eq 2049 log
access-list 101 permit udp any 192.9.200.0 0.0.0.255 gt 1023

end
```