

Administration et sécurité des réseaux

TD : Filtrage

Pour des raisons de sécurité et d'organisation, l'architecture du réseau d'une entreprise a été conçue comme indiqué dans la figure 1.

- Le réseau LAN-1 est le réseau des serveurs accessibles de l'extérieur et de l'intérieur de l'entreprise
- Le réseau LAN-2 est le réseau de la direction générale
- Le réseau LAN-3 est le réseau du personnel

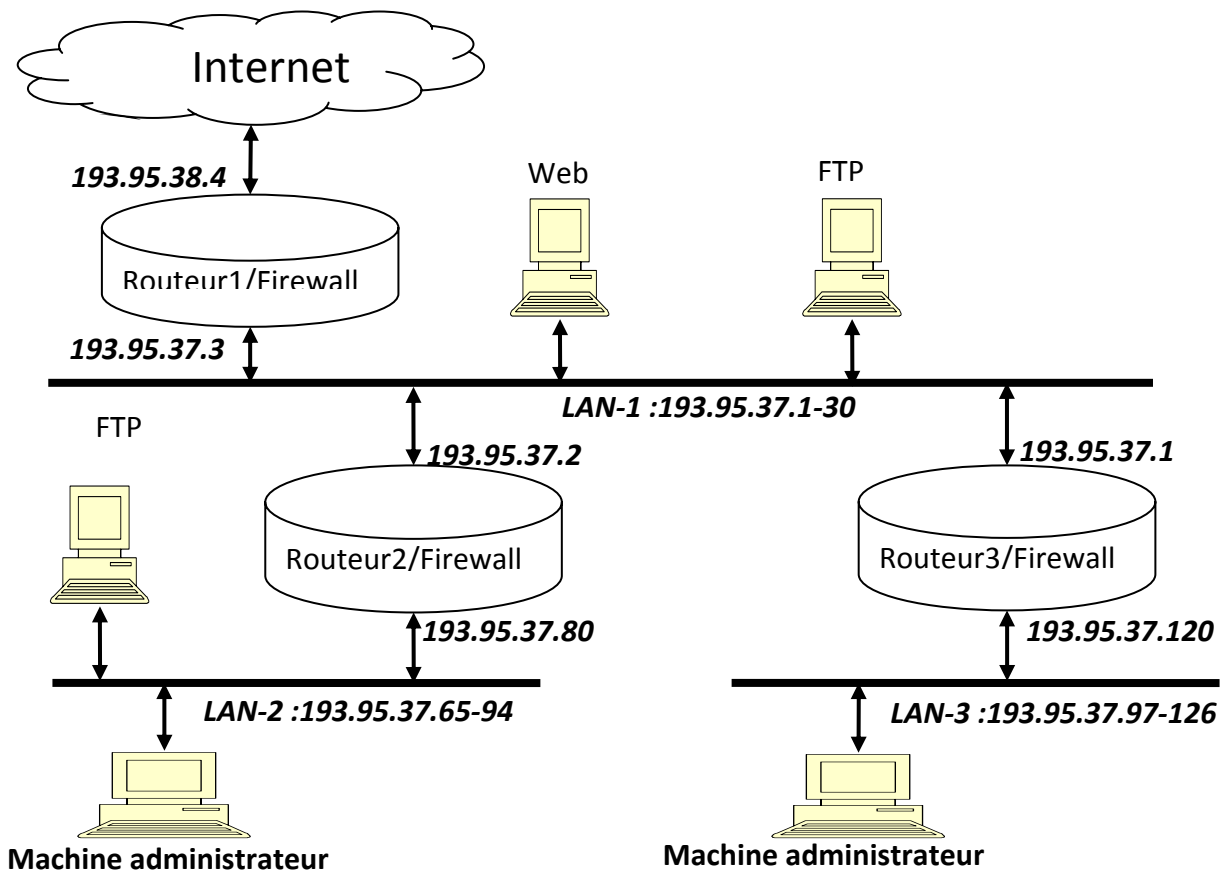


Figure 1 : architecture du réseau

Question : Donner et ordonner les règles de filtrage sur chaque routeur permettant de répondre à la politique de sécurité suivante (présentée par les règles A, B, C et D):

- Autoriser uniquement les machines administrateurs d'adresses IP 193.95.37.65 et 193.95.37.100 à lancer la commande *echo* (port 7 UDP(17)) sur toutes les machines de l'entreprise. Toutes les tentatives de lancer ces commandes à partir de l'extérieur seront bloquées.
- Permettre l'échange de trafic TCP (6) entre le LAN-1 et le LAN-3.
- Permettre uniquement à la machine externe d'adresse 103.95.40.40 d'envoyer un trafic ICMP (1) sur toutes les machines du réseau de l'entreprise (LAN-1, LAN-2 et LAN-3)
- Interdire l'échange de trafic FTP (port 21, TCP) entre le LAN-1 et le LAN-3

N.B :

- Répondre dans les tableaux ci-dessous en se limitant aux champs présentés.
- Une case vide signifie que cette dernière peut prendre n'importe quelle valeur

Routeur 1

N° de la règle	Interface d'arrivée	@IP source	Port source	@IP dest	port dest	Nom ou N° du protocole	Nom de la règle	Action
1	.4	Toutes	>1023	LAN1, LAN2, LAN3	7	UDP	A	Bloquer
2	.38.4	.40.40	NA	LAN1, LAN2, LAN3	NA	ICMP	C	Accepter
3	.37.3	LAN1 LAN2 LAN3	NA	.40.40	NA	ICMP	C	Accepter

Routeur 2

N° de la règle	Interface d'arrivée	@IP source	Port source	@IP dest	port dest	Nom ou N° du protocole	Nom de la règle	Action
1	.80	.65	>1023	.37.0 et .37.96	7	UDP	A	Accepter
2	.2	.37.0 et .37.96	7	.65	>1023	UDP	A	Accepter
3	.2	.100	>1023	.37.64	7	UDP	A	Accepter
4	.80	.37.64	7	.100	>1023	UDP	A	Accepter
5	.2	.40.40	NA	LAN2	NA	ICMP	C	Accepter
6	.80	.37.64	NA	.40.40	NA	ICMP	C	Accepter

Routeur 3

N° de la règle	Interface d'arrivée	@IP source	Port source	@IP dest	port dest	Nom ou N° du protocole	Nom de la règle	Action
1	.1	.65	>1023	.37.96	7	UDP	A	Accepter
2	.120	.37.96	7	.65	>1023	UDP	A	Accepter
3	.120	.100	>1023	.37.0 et.37.64	7	UDP	A	Accepter
4	.1	.37.0 et.37.64	7	.100	>1023	UDP	A	Accepter
5	.1	.40.40	NA	LAN3	NA	ICMP	C	Accepter
6	.120	.37.96	NA	.40.40	NA	ICMP	C	Accepter
9	.1	LAN1	tous	LAN2	tous	TCP	B	Accepter
10	.120	LAN2	tous	LAN1	tous	TCP	B	Accepter
7	.1	LAN1	>1023	LAN3	21	TCP	D	Bloquer
8	.120	LAN3	>1023	LAN1	21	TCP	D	Bloquer