Exercice1 :

Une entreprise dispose d'un pare-feu pour limiter l'accès depuis et vers les machines de son réseau interne. L'architecture du réseau de l'entreprise comprend également une zone démilitarisée (DMZ) pour le déploiement des serveurs Web et DNS propres à l'entreprise. La politique de sécurité appliquée par le pare-feu est décrite par le tableau 1.

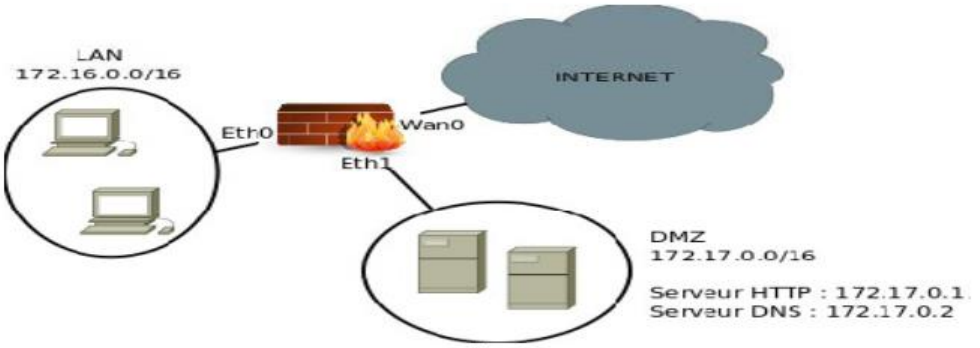

tableau 1

tableau 1

N°	Interface entrée	Interface sortie	Adr IP source	Adr IP destination	Protocole	Port source	Port dest	Action
1	Eth0	Eth1	172.16.0.0	172.17.0.1	TCP	> 1024	80	Accepter
2	Eth1	Eth0	172.17.0.1	172.16.0.0	TCP	80	> 1024	Accepter
3	Eth0	Eth1	172.16.0.0	172.17.0.2	UDP	> 1024	53	Accepter
4	Eth1	Eth0	172.17.0. 2	172.16.0.0	UDP	53	> 1024	Accepter
5	Wan0	Eth1	*	172.17.0.1	TCP	> 1024	80	Accepter
6	Eth1	Wan0	172.17.0.1	*	TCP	80	> 1024	Accepter
7	Eth0	Wan0	172.16.0.0	*	TCP	> 1024	80	Accepter
8	Wan0	Eth0	*	172.16.0.0	TCP	80	> 1024	Accepter
9	*	*	*	*	*	*	*	Refuser

1) Donner la politique correspondante à chaque paire de règles (1-2), (3-4), (5-6) et (7-8)
2) Préciser la règle qui vérifiera chacun des paquets suivants et dites si le paquet sera accepté ou refusé

p1-	IP sce : 172.16.0.30	IP Dest : 12.230.24.45	Prot : TCP	Port sce :1045	Port dest : 443
p2-	IP sce : 172.16.10.5	IP Dest : 172.17.0.2	Prot : UDP	Port sce :6810	Port dest : 53
p3-	IP sce : 140.10.2.1	IP Dest : 172.17.0.1	Prot : TCP	Port sce :8000	Port dest : 80
p4-	IP sce : 17.14.3.3	IP Dest : 172.17.0.2	Prot : UDP	Port sce :6000	Port dest : 53
p5-	IP sce : 172.17.0.1	IP Dest : 1.2.3.4	Prot : TCP	Port sce :80	Port dest : 9999

Exercice 2 :

Soit l'architecture du réseau indiqué dans la figure 1 où LAN1 est le réseau des serveurs accessibles de l'extérieur et de l'intérieur de l'entreprise

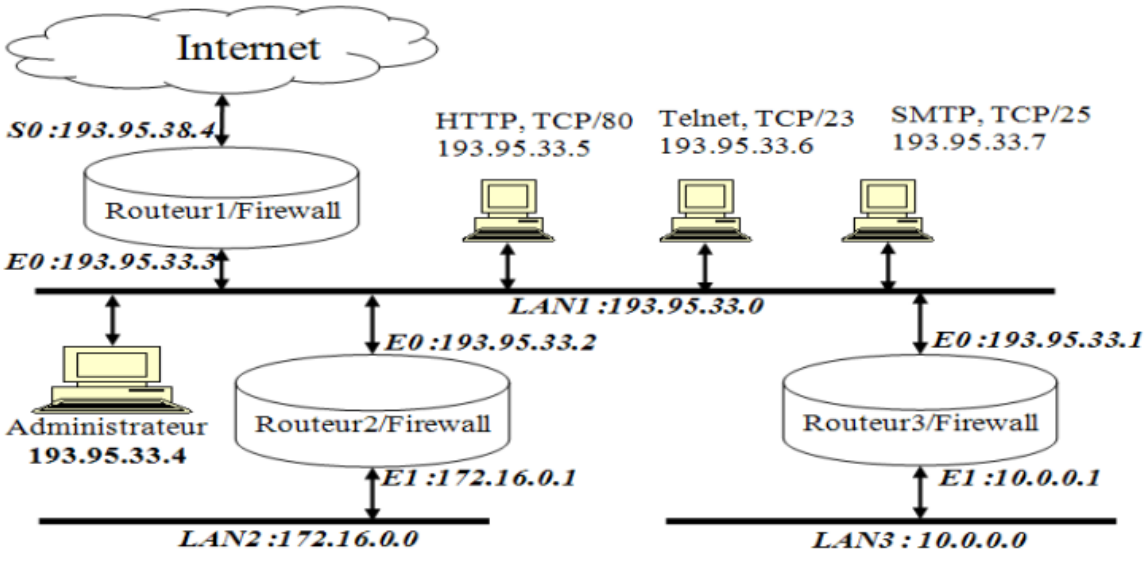

Figure 1 : architecture du réseau

1) Dans quels routeurs doit-on implémenter des règles de filtrage dans chacun des cas suivants (répondre par oui ou non):

	Routeur1	Routeur2	Routeur3
Permettre aux utilisateurs internes et externes d'accéder aux serveurs HTTP, FTP et SMTP du LAN1.			
Permettre à la machine administrateur d'accéder aux différents LAN.			
Permettre aux utilisateurx du LAN1 d'accéder à Internet			

2) Compléter le tableau suivant permettant aux utilisateurs externes d'accéder au serveur http du LAN1 et permettant aux utilisateurs du LAN1 d'accéder aux serveurs web externes.

@IP source	@IP dest	Port source	Port destination	Protocole	ACK=1	Action

Exercice 3:

Fabrication des clés par RSA

L'utilisateur A choisit les facteurs premiers p = 11 et q = 23. Trouvez n, e et d et les clé publique et privé

Utilisant la valeur de n trouvée dans l'exercice 1 et e, déterminez l'espace des messages en clair {0, 1, …, n-1}. Puis chiffrez le message m = 165 noté c.

Utilisant les valeurs de n, d et e trouvées dans l'exercice 1, déterminez à partir du message c précédent le message m.

Corrigés

Exercice 1 :

1)

règles	*politique*
(1,2)	Permettre aux utilisateurs du RL d'accéder au serveur HTTP local
(3,4)	Permettre aux utilisateurs du RL d'accéder au serveur DNS local
(5,6)	Permettre aux utilisateurs externes d'accéder au serveur HTTP local
(7,8)	Permettre aux utilisateurs du RL d'accéder aux serveurs HTTP sur Internet

2)

paquet	N° de la règle à appliquer (d'après le tableau 1)	Action (accepter ou refuser)
P1	9	refusé
P2	3	accepté
P3	5	accepté
P4	9	refusé
P5	6	accepté

Exercice 2 :

1)

	Routeur1	Routeur2	Routeur3
Permettre aux utilisateurs internes et externes d'accéder aux serveurs HTTP, FTP et SMTP du LAN1.	x	x	x
Permettre à la machine administrateur d'accéder aux différents LAN.		x	x
Permettre aux utilisateurs du LAN1 d'accéder à Internet	x		

2)

@IP source	@IP dest	Port source	Port destination	Protocole	ACK=1	Action
*	193.95.33.5	>1023	80	TCP	*	accepter
193.95.33.5	*	80	>1023	TCP	oui	accepter
193.95.33.0	*	>1023	80	TCP	*	accepter
*	193.95.33.0	80	>1023	TCP	oui	accepter

Exercice 3 :

Puisque les deux nombres 11 et 23 sont premiers entre eux, alors n est calculé par le produit
n = p q = 11*23 =253.
2- Il faut choisir un entier e le plut petit tel que :
$1 < e < \Phi(253) = (p-1)(q-1) = (11-1)(23-1) = 220$ et PGCD(e, (p-1)(q-1)) =1

d'où, on peut choisir e =3, car PGCD(3, 220) = 1.
3- L'entier d est calculé avec les conditions suivantes :
$1 < d < (p-1)(q-1)$ et de =1 mod (p-1)(q-1)
On utilisant l'algorithme d'Euclide étendu la valeur de d est 147.
Donc la clé publique de A est Kp = (e, n) et sa clé privée est Kpr = (d, n). Après il détruit les nombres p, q et $\Phi(253)$.

L'espace des messages en clair est constitué de tous les messages m avec 0<= m <n. Le message en clair m est chiffré par la relation c = m^e mod n.
Pour m = 165, on obtient c = 165^3 mod 253 = 110.

De la même manière que l'exercice 2, le message c est déchiffré par la relation 110^147 mod 253 = 165.