

Examen

Administration et sécurité des réseaux

Classes: 3SIL

Exercice 1 [7pts]: Soit l'architecture du réseau 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

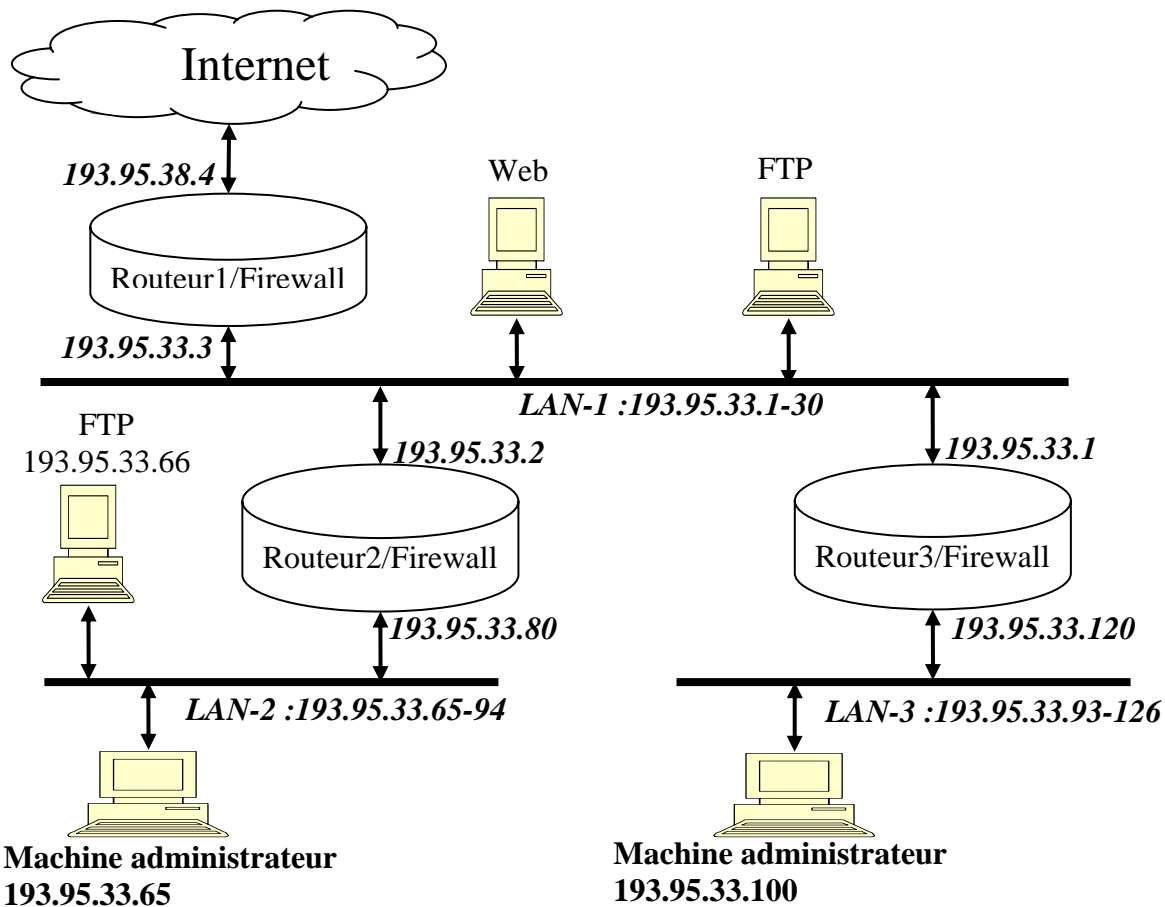


Figure 1 : architecture du réseau

Question1 : Pour permettre aux utilisateurs des réseaux LAN-1, LAN-2 et LAN-3 à dialoguer avec des serveurs SMTP externe, les règles suivantes ont été définies au niveau des trois routeurs du réseau de l'entreprise. Expliquer pourquoi ces règles peuvent permettre à un agresseur de lancer des attaques sur les réseaux de l'entreprise? Proposer une solution : de nouvelles règles de filtrage.

Routeur 1, 2 et 3	IP source	IP destination	Protocole et port source	Protocole et port destination	Action
Paquet entrant	Toutes	Toutes	TCP/25	Toutes	Autoriser
Paquet sortant	Toutes	Toutes	Toutes	TCP/25	Autoriser

Question2 : 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) en se limitant aux champs suivants:

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
----------------	---------------------	------------	-------------	----------	-----------	------------------------	-----------------	--------

- A. Autoriser **uniquement** la machine administrateur 193.95.33.65 à lancer la commande **telnet** (port 23 TCP (6)) sur toutes les machines de l'entreprise. Toutes les tentatives de lancer cette commande à partir de l'extérieur seront bloquées.
- B. Permettre l'échange de trafic TCP (6) entre le LAN-1 et le LAN-2.
- C. Permettre uniquement à la machine externe d'adresse 103.95.11.11 d'envoyer un trafic ICMP (1) sur **uniquement** les machines du LAN1.
- D. Interdire l'échange de trafic FTP (port 21, TCP(6)) entre le LAN-1 et le LAN-2

Exercice 2[6pts]:

- Donner l'utilité d'un DNS cache ?
- Un DNS secondaire peut-il contenir plus d'information de résolution de noms que son DNS primaire
- Une zone peut-elle être gérée par un seul serveur DNS?
- Soient les deux messages DNS suivants représentant une requête et sa réponse :

```

Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 (Standard query response, No error)
 1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... .0... .. = Authoritative: Server is not an authority for domain
... ..0... .. = Truncated: Message is not truncated
... ..1... .. = Recursion desired: Do query recursively
... ..1... .. = Recursion available: Server can do recursive queries
... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
... ..0000 = Reply code: No error (0)
Questions:
Answer RRs:
Authority RRs:
Additional RRs:
Queries
Answers
  www.ibm.com: type A, class inet, addr 129.42.16.99
  www.ibm.com: type A, class inet, addr 129.42.17.99
  www.ibm.com: tvbe A. class inet. addr 129.42.18.99
Authoritative nameservers
  ibm.com: type NS, class inet, ns NS.AUSTIN.ibm.com
  ibm.com: type NS, class inet, ns NS.WATSON.ibm.com

```

```

Domain Name System (query)
Transaction ID: 0x0002
Flags: 0x0100 (Standard query)
 0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... ..0... .. = Truncated: Message is not truncated
... ..1... .. = Recursion desired: Do query recursively
... ..0... .. = Non-authenticated data OK: Non-authenticated data is unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.ibm.com: type A, class inet
    Name: www.ibm.com
    Type: Host address
    Class: inet

```

- Compléter les quatre champs manquants dans le premier message
- S'agit-il d'une requête standard ou inverse? Expliquer
- Le message réponse provient-il d'un serveur DNS primaire? Expliquer

Exercice 3 [7pts]:

Une technique de chiffrement simple consiste à effectuer le "ou exclusif \oplus " du message m à chiffrer avec une clé k qui est aussi longue que le message à protéger. On note $m \oplus k$ le message m chiffré avec k , si $m[i]$ est le $i^{\text{ème}}$ bit du message m et $k[i]$ est le $i^{\text{ème}}$ bit de la clé k , alors le $i^{\text{ème}}$ bit de $m \oplus k$ est égal à $(m[i] \oplus k[i])$.

- 1- Qu'appelle-t-on technique de chiffrement symétrique?
- 2- Montrez que le "ou exclusif \oplus " est une technique de chiffrement symétrique.
- 3- Cette technique est difficilement applicable car le fait de stocker des clés secrètes aussi longues que les messages n'est pas très pratique. En revanche, il est possible de générer un message aléatoire N de la même taille que le message à chiffrer. Dans le premier protocole, c'est le service S qui génère N et l'envoi à X et Y , dans le second protocole c'est X qui génère N_X et Y qui génère N_Y .

Protocole 1

- $S \rightarrow X, Y: N$
- $X \rightarrow Y: m \oplus N$

Protocole 2

- $X \rightarrow Y: m \oplus N_X$
- $Y \rightarrow X: m \oplus N_X \oplus N_Y$
- $X \rightarrow Y: m \oplus N_Y$

Analysez les 2 protocoles du point de vue de X , Y et de Z un participant malveillant qui peut écouter tous les messages échangés, en expliquant les messages transférés entre X et Y .

Est-ce que ces protocoles permettent à X et Y d'échanger de façon confidentielle le message m ? Expliquer?

Rappel : Quelques propriétés mathématiques

$$A \oplus B = \bar{A}.B + A.\bar{B}$$

$$\overline{A \oplus B} = A.B + \bar{A}.\bar{B}$$

$$A \oplus A = 0$$

$$A \oplus 0 = A$$

$$A \oplus 1 = \bar{A}$$

$$A \oplus \bar{A} = 1$$