Correction TD

Exo2

1. *Le protocole SSL avec un certificat serveur offre d'abord une authentification du partenaire accédé par une vérification que ce serveur détient bien la clef privée correspondant à la clef publique diffusée. Ensuite, la communication est chiffrée, on a donc des garanties sur la confidentialité des échanges ainsi que sur l'intégrité de la communication pendant toute sa durée.*

Exo2

2. *Le certificat n'inclut pas seulement la clef publique, mais également une signature de cette clef publique par un autre certificat. (Celui-ci pouvant également être un certificat intermédiaire.) La racine de cette chaîne de certification doit être un certificat pré-installé sur le navigateur (ou obtenu indépendamment en préalable à la communication). L'utilisateur peut alors être sûr que le certificat diffusé par le serveur appartient bien à l'organisme indiqué s'il vérifie la chaine de certification, s'il a confiance dans le certificat racine et s'il a confiance dans les organismes détenteurs des certificats intermédiaires pour avoir fait les vérifications nécessaires avant de signer les certificats dérivés. (Il s'agit alors de tiers de confiance ou d'autorités de certification.)*

Exo2

3. *Le certificat serveur n'offre qu'une authentification du serveur. Si le service accédé gère une base de comptes utilisateurs, ceux-ci doivent donc également en plus s'authentifier. Cette authentification du client peut éventuellement s'effectuer via un nom d'utilisateur et un mot de passe. Cette méthode est moins forte qu'une technique faisant appel à des algorithmes de cryptographie asymétriques, mais elle est bénéficie néanmoins via HTTPS de la protection offerte par le canal chiffré et signé de SSL.*

Exo2

4. *Dans ce cas, l'authentification du client, appuyée sur un certificat et une authentification à clef privée/clef publique offre des garanties bien plus importantes en terme de sécurité. Par contre, il faut alors gérer une procédure de délivrance de ces certificats clients (incluant leur signature par un tiers de confiance, après vérification de l'identité du demandeur par exemple).*

Exo2

5. *La clef privée associée à un certificat ne doit être que très rarement stockée en clair (notamment sur disque). Elle est protégée par un chiffrement symétrique dont la « passphrase » constitue la clef. C'est donc un mot de passe permettant de déverrouiller l'usage du certificat et de protéger la clef privée de l'utilisateur en cas de vol (par exemple afin de lui laisser le temps de détecter le vol et de révoquer son certificat).*

4.1

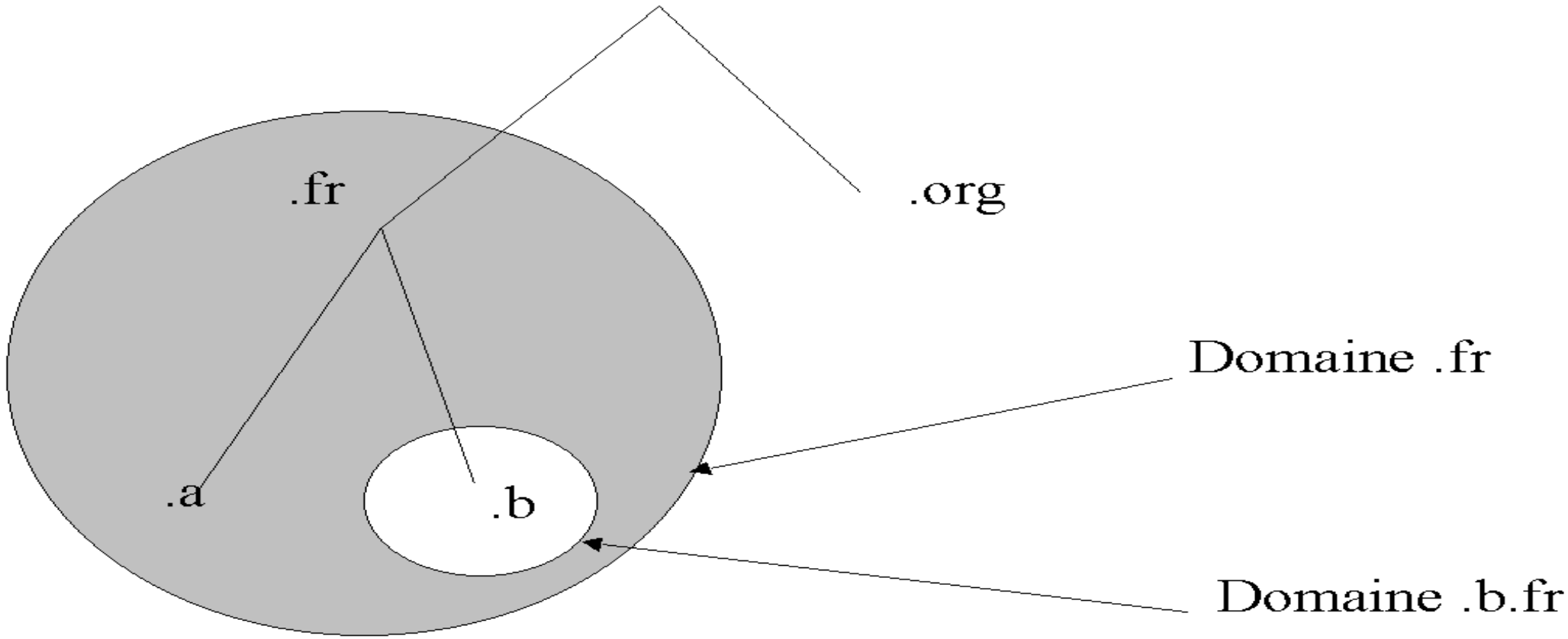
Question 1:

- *La DMZ Admin est une zone d'administration des équipements de sécurité. Elle contient un serveur de gestion des firewall qui stocke également les traces que ces équipements collectent. On trouve également dans cette zone un serveur DNS, probablement placé là car il s'agit d'une zone de haut niveau de sécurité. Ce serveur DNS est alors probablement le serveur principal des zones attribuées à l'entreprise ou l'organisme concerné.*
- *La DMZ contient un serveur Web accessible de l'extérieur. Elle contient également un relais HTTP, qui doit servir à relayer les accès internes vers Internet.*
- *La zone « salle serveurs » est elle aussi placée dans une zone de sécurité spécifique. Ainsi, l'ensemble des serveurs sont logiquement isolés au niveau du réseau des postes de travail et des autres zones de sécurité.*

4.2

On peut supposer que le serveur DNS de la DMZ Admin. correspond au serveur DNS visible sur Internet qui gère en propre la zone DNS de l'entreprise. Par contre, le serveur DNS associé au serveur AD situé en interne gère également des zones de nommage (via le DNS) mais qui sont associées aux machines internes du LAN (noms de machines Windows, noms de domaines, etc.). Cette zone n'est a priori pas visible depuis Internet.
Par contre, on entrevoit là une difficulté de fonctionnement. En effet, les postes de travail peuvent avoir besoin d'accéder simultanément aux deux zones de nommage et la configuration respective des deux serveurs sera à étudier plus précisément (notamment si on souhaite éviter que tous les clients n'aient à essayer la résolution de leurs noms auprès des deux serveurs tour à tour, ce qui n'est pas vraiment optimal).

-4.2’



4.3

- A)

En terme de protection, on dispose ici de deux lignes de défense pour les éléments de l'organisme ayant très probablement le plus de valeur dans le système d'information: ses serveurs internes. C'est certainement positif du point de vue de la sécurité si les firewall sont gérés correctement.
Un point d'administration central est également prévu, qui semble donc ainsi offrir des fonctions de gestion unifiée des 2 équipements afin de faciliter leur configuration. Toutefois, on imagine déjà que cette configuration sera plus compliquée qu'avec un seul équipement faisant face seulement à des flux à la frontière avec Internet.

4.3

- B)

Le firewall externe est exposé à l'ensemble d'Internet. Il est donc susceptible de faire face à des menaces extrêmement variées. Par contre, les protocoles qui le traversent sont probablement peu nombreux et relativement faciles à préciser et maitriser. C'est finalement un cas assez classique d'utilisation de ce genre d'équipement.
Le firewall interne est essentiellement destiné à assurer une protection des serveurs vis à vis des utilisateurs internes (ou en 2° ligne de protection pour une intrusion externe réussie sur les postes de travail). Or, en interne au LAN, les flux réseaux sont parfois très variés (impression, partage de fichiers, etc.) et la configuration de ce firewall va sans doute être difficile à affiner précisément. On sera même surement amené à faire des compromis sur cette configuration afin d'éviter des dysfonctionnements. Par ailleurs, la volumétrie des flux réseaux concernés sera certainement beaucoup plus importante sur le LAN au niveau du firewall interne que vis à vis d'Internet. La performance de cet équipement sera donc à surveiller.

4.4

La DMZ d'administration peut être vue comme la zone de plus haut niveau de sécurité dans l'architecture. Il aurait peut-être été plus logique dans ce cas de la faire elle aussi bénéficier du double niveau de protection réseau (tout comme les serveurs). On aurait donc pu raccorder cette DMZ d'administration sur le 2° firewall interne au lieu de la connecter directement au 1° firewall.
(Par contre, dans ce cas, le positionnement du serveur DNS serait à ré-étudier.)

Peut-être le firewall interne a t'il été installé dans un 2° temps, après que le firewall tourné vers Internet ait été déployé ?

4.5

Si les deux firewall sont identiques, on note déjà un risque en cas de faille de sécurité sur l'équipement en question. L'avantage d'avoir deux firewall différents, c'est que même en cas de vulnérabilité grave affectant le firewall en contact avec Internet, le 2° équipement interne pourra assurer une protection des principaux serveurs.
Par contre, en terme de configuration, il sera alors certainement très difficile de disposer d'un moyen de configuration unifié des deux équipements. On aura donc un inconvénient (probablement important) vis à vis de la facilité d'administration de l'architecture.

Exemple de script

```
#!/bin/sh

# Réinitialise les règles
sudo iptables -t filter -F
sudo iptables -t filter -X

# Bloque tout le trafic
sudo iptables -t filter -P INPUT DROP
sudo iptables -t filter -P FORWARD DROP
sudo iptables -t filter -P OUTPUT DROP

# Autorise les connexions déjà établies et localhost
sudo iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -t filter -A INPUT -i lo -j ACCEPT
sudo iptables -t filter -A OUTPUT -o lo -j ACCEPT

# ICMP (Ping)
sudo iptables -t filter -A INPUT -p icmp -j ACCEPT
sudo iptables -t filter -A OUTPUT -p icmp -j ACCEPT

# SSH
sudo iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT

# DNS
sudo iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
sudo iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

# HTTP
sudo iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

# FTP
sudo iptables -t filter -A OUTPUT -p tcp --dport 20:21 -j ACCEPT
sudo iptables -t filter -A INPUT -p tcp --dport 20:21 -j ACCEPT

# Mail SMTP
iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 25 -j ACCEPT

# Mail POP3
iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 110 -j ACCEPT

# Mail IMAP
iptables -t filter -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 143 -j ACCEPT

# NTP (horloge du serveur)
sudo iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT
```

TD2

- iptables -t filter -A (chain) -p (protocole) --dport (port_a_ouvrir) –j (décision)
  - Exemple

```
# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
```

Cela ajoute à la section `INPUT` (donc, pour le trafic entrant) une règle sur les données reçues via le protocole TCP sur le port de `ssh` (vous pouvez remplacer `ssh` par le numéro du port, soit 22). Lorsque votre ordinateur recevra des données en TCP sur le port de SSH, celles-ci seront acceptées ; cela vous permettra donc de vous connecter à distance à votre PC via SSH.

Vous pouvez faire de même avec d'autres ports :

console

```
# iptables -A INPUT -p tcp --dport www -j ACCEPT
```

… pour le web (80).

console

```
# iptables -A INPUT -p tcp --dport imap2 -j ACCEPT
```

… pour les mails, etc.

service	port d'écoute	protocole
ssh	22	tcp
web/HTTP	80	tcp
FTP	20 et 21	tcp
mail/SMTP	25	tcp
mail/POP3	110	tcp
mail/IMAP	143	tcp
DNS	53	tcp et udp

TD2-2013

- Remarques:
  - Pesez au trafic aller(requête) et retour(réponse).
  - Pensez au mode de communication clients (requêtes)– serveur(réponses)
  - Soyez le plus précis possible sur les paramètres

TD2-Exercice 1

- a) La chaines de filtrages INPUT représente les messages à destination du pare-feu(processus locaux)
- b) La chaines de filetrage OUTPUT représente les messages en provenances du pare-feu(processus locaux)
- c) La chaines de filtrages FORWARD représente les messages routés, CAD les messages dont le pare-feu n'est ni la source ni la destination.
- d) Demande de conecxion TCP(CAD le message initial du lient avec le drapeau TCP SYN): *-m conntrack –ctstate NEW*
- Connexion établie TCP (CAD les messages du client et du serveur après la connection) : *-m conntrack –ctstate ESTABLISED*

TD2-Exercice 2

- A)
  - Innitialisation

  iptables –F

  iptables –x

  iptables –Z
  - Politique par défaut

  iptables –P INPUT DROP

  iptables –P OUTPUT DROP

  iptables –P FORWARD DROP

TD2-Exercice 2

- B)
  - ❖Autoriser le LAN 1 à accéder à Internet

  iptables –A FORWARD –i eth0 –s 192.168.10.0/24 –o eth3 –j ACCEPT

  iptables –A FORWARD –o eth0 –d 192.168.10.0/24 –i eth3 –j ACCEPT

TD2-Exercice 2

- C)
  - ❖Autoriser le PC 2 à accéder à Internet

    iptables –A FORWARD –i eth1 –s 192.168.10.20 –o eth3 –j ACCEPT

    iptables –A FORWARD –o eth1 –d 192.168.10.20 –i eth3 –j ACCEPT

TD2-Exercice 2

- d)
  - ❖Autoriser les requêtes ping à destination du pare-feu

  iptables –A INPUT –p icmp - - icmp-type echo-request –j ACCEPT

  iptables –A OUTPUT –p icmp - - icmp-type echo-reply –j ACCEPT

TD2-Exercice 3

- A)
  - Innitialisation

  iptables –F

  iptables –x

  iptables –Z
  - Politique par défaut

  iptables –P INPUT DROP

  iptables –P OUTPUT DROP

  iptables –P FORWARD DROP

TD2-Exercice 3

- B)
  - ❖Autoriser le LAN à naviguer sur le Web (HTTP,HTTPS,DNS)

  iptables –A FORWARD –p tcp –i eth0 –s 172.16.10.0/24 –o eth3 –m multiport - - dports 80,443 –m conntrack - - ctstate NEW, ESTABLISHED –j ACCEPT

  iptables –A FORWARD –p utp –i eth0 –s 172.16.10.0/24 –o eth3 - - dports 53 –m conntrack - - ctstate ESTABLISHED –j ACCEPT

  iptables –A FORWARD –p tcp –o eth0 –d 172.16.10.0/24 –i eth3 –m multiport - - sports 80,443 –m conntrack - - ctstate NEW, ESTABLISHED –j ACCEPT

  iptables –A FORWARD –p utp –o eth0 –d 172.16.10.0/24 –i eth3 - - sports 53 –m conntrack - - ctstate ESTABLISHED –j ACCEPT

TD2-Exercice 3

- c)
  - ❖Autoriser les connexions http à destination du serveur de la DMZ

  iptables –A FORWARD –p tcp –o eth1 –d 172.16.11.1 - - dports 80 –m conntrack - - ctstate NEW, ESTABLISHED –j ACCEPT

  iptables –A FORWARD –p tcp –i eth1 –s 172.16.11.1 - - sports 80 –m conntrack - - ctstate ESTABLISHED –j ACCEPT

TD2-Exercice 3

- d)
  - ❖Autoriser les requetes ping à destination du serveur de la DMZ

    iptables –A FORWARD –p icmp –o eth1 –d 172.16.11.1 - - icmp-type echo-request –j ACCEPT

    iptables –A FORWARD –p icmp –i eth1 –s 172.16.11.1 - - icmp-type echo-reply –j ACCEPT

TD2-Exercice 3

- e)
  - ❖Autoriser les PC1 à se connecter en SSH sur le serveur de la DMZ

    iptables –A FORWARD –p tcp –i etho –s 172.16.10.10 –o eth1 –d 172.16.11.1 - -dport 22 –m conntrack - -ctstate NEW, ESTABLISHED –j ACCEPT

    iptables –A FORWARD –p tcp –o etho –d 172.16.10.10 –i eth1 –s 172.16.11.1 - -sport 22 –m conntrack - -ctstate ESTABLISHED –j ACCEPT