Université de Limoges — FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

Infrastructure Réseaux

Examen — mai 2015

Durée : 1h30 — Documents autorisés

MPLS — 2 points

1 – 2pts

a. Comparez une solution MPLS et un VPN de type IPSec : donnez les avantages et inconvénients de ces deux technologies. *(1pt)*

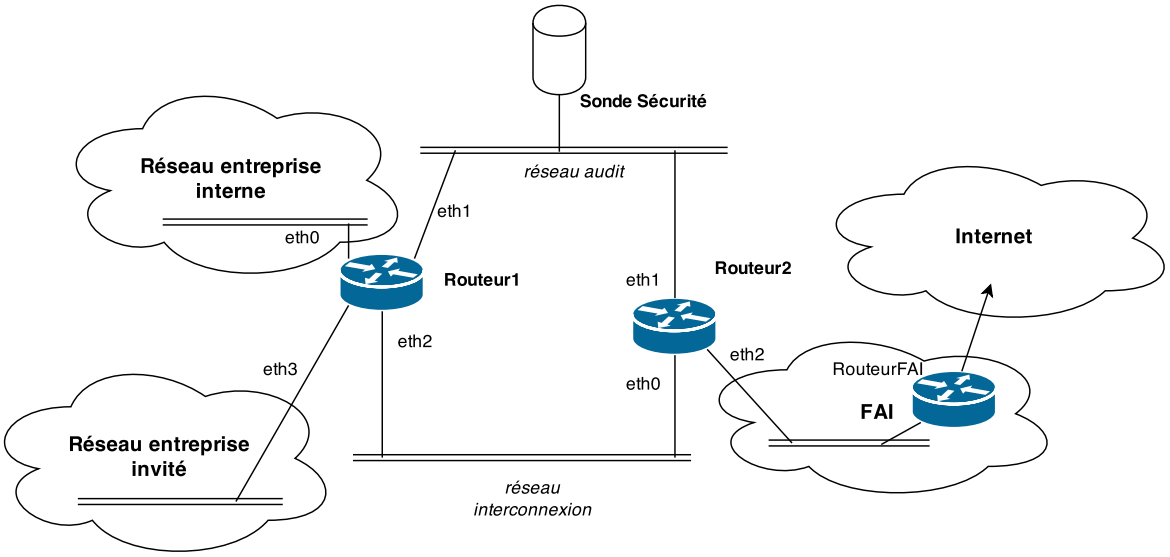
b. Peut-on utiliser un routeur non MPLS dans un réseau d'interconnexion de routeurs à la place d'un routeur MPLS ? Pourquoi ? *(1pt)*

Policy Routing & Firewall — 16 points

2 – 7pts Une entreprise possède un réseau décomposé en differents sous-réseaux :

- ☐ « interne » configuré en `193.58.13.128/25` ;
- ☐ « audit » configuré en `10.0.7.0/24` ;
- ☐ « invité » configuré en `163.19.34.0/25` ;
- ☐ « interconnexion » en `192.168.87.0/24` ;

Elle se connecte au réseau de son FAI avec l'adresse `164.87.34.253` dans le réseau `164.87.0.0/16`.



Routeur 1 :
- `eth0:193.58.13.254`
- `eth1:10.0.7.254`
- `eth2:192.168.87.254`
- `eth3:163.19.34.126`

Routeur 2 :
- `eth0:192.168.87.253`
- `eth1:10.0.7.253`
- `eth2:164.87.34.253`

Routeur FAI :
- `eth0:164.87.34.254`

Pour assurer la surveillance des communications en provenance du réseau « invité », elle a déployé une « sonde », c-à-d un serveur hébergeant différents outils de surveillance et de détection d'intrusion, et capable de *sniffer* tous les paquets passant dans le réseau « audit ».
Le trafic du réseau « interne » qui ne doit pas être surveillé, passe par le réseau « interconnexion ».

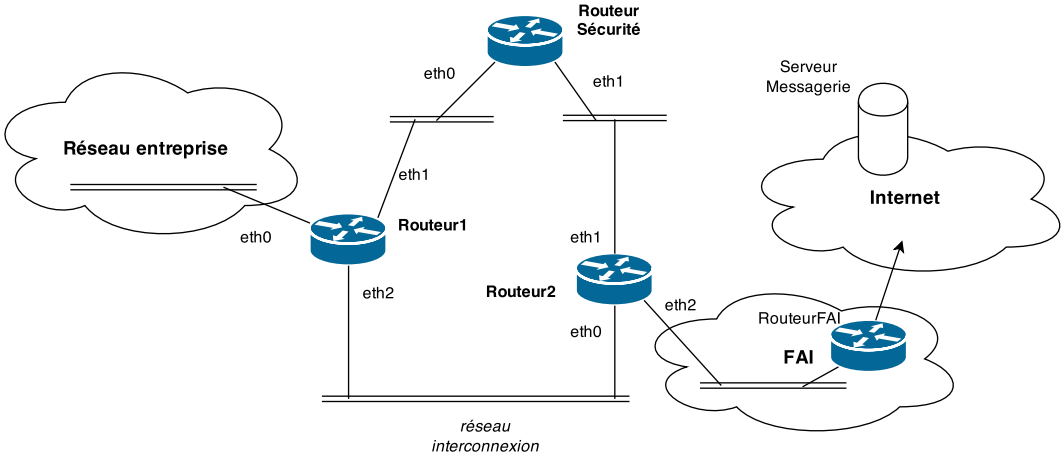
Questions :

a. Que faut-il utiliser : de la « Policy Routing » et/ou du « firewall » ? *(1pt)*
Vous justifierez votre réponse.

b. Donnez la configuration de Routeur 1 permettant aux trafic en provenance du réseau « invité » de passer par le réseau « audit » pour aller sur Internet. *(4pts)*

c. Donnez la configuration de Routeur 2 permettant au trafic en retour d'Internet d'atteindre les réseaux « interne » et « invité » respectivement. *(2pts)*

3 – 9pts Une entreprise utilise une solution de messagerie externalisée. Elle veut sécuriser l'envoi et la réception de ses messages en faisant passer le trafic à **destination et en provenance** du « serveur de messagerie » au travers d'un routeur disposant d'outils d'anti-virus, d'analyse de SPAM et de filtrage de contenu sensible (secrets de fabrication, commandes fournisseurs *etc*).
Ces outils de sécurité contenant des informations sensibles, elle ne peut souscrire à l'offre de sécurité offert par le serveur de messagerie.



Routeur 1 :
- `eth0:145.78.34.254`
- `eth1:10.0.0.254`
- `eth2:192.168.0.254`

Routeur Sécurisé :
- `eth0:10.0.0.253`
- `eth1:172.16.0.253`

Routeur 2 :
- `eth0:192.168.0.253`
- `eth1:172.16.0.254`
- `eth2:67.12.78.254`

Le réseau de l'entreprise est le `145.78.34.0/24`.
L'adresse du serveur de messagerie est `164.81.1.10`.
Les protocoles de messagerie à considérer sont le SMTP (TCP, 25) et l'IMAP (TCP,143).
Le réseau FAI est en `67.12.0.0/16` et le routeur FAI est en `67.12.78.128`.
Le trafic du réseau entreprise, autre que lié à la messagerie, passe par défaut par le réseau « interconnexion ».

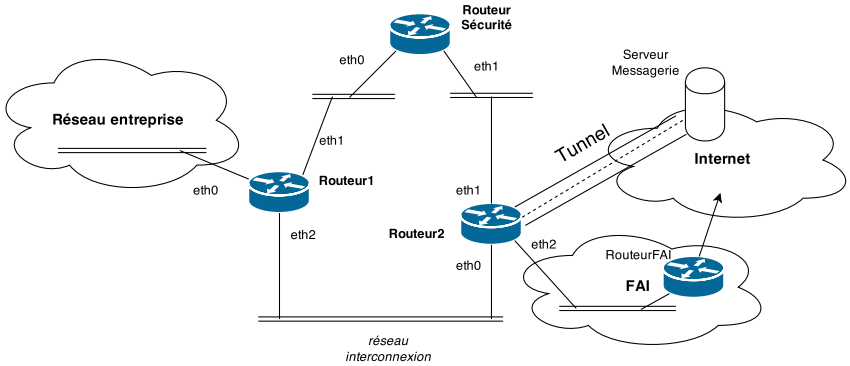
Questions :

a. Que faut-il utiliser : de la « Policy Routing » et/ou du « firewall » ? *(1pt)*
Vous justifierez votre réponse.

b. Est-ce que le traitement du trafic à destination du serveur de messagerie est différent de celui du trafic en provenance du serveur de messagerie ? *(1pt)*

c. Donnez la configuration de « Routeur 1 » et de « Routeur 2 » permettant au trafic vers et depuis la messagerie de passer par le « Routeur Sécurité » *(4pts)*

L'entreprise voudrait sécuriser le trafic à la sortie de Routeur 2 (elle ne peut pas le faire à l'intérieur pour permettre aux outils de surveillance d'intercepter le contenu du trafic).
Pour cela elle met en place un tunnel GRE/IPSec avec le serveur de messagerie :



d. Donnez les modifications à apporter à votre configuration précédente pour que seul le trafic à destination du serveur de messagerie passe par le tunnel. *(3pts)*
Vous choisirez une configuration IP pour le tunnel. La configuration sur le serveur de messagerie n'est pas à donner.

▬▬▬ Routage dynamique & « *Routing Protocol* » — 2 points

4 – 2pts Dans un réseau d'interconnexion on a capturé le trafic suivant :

```
05:06:26.942558 IP (tos 0xc0, ttl 2, id 0, offset 0, flags [none], proto UDP (17), length 112)
    10.0.0.1.520 > 224.0.0.9.520: [udp sum ok]
   RIPv2, Response, length: 84, routes: 4 or less
     AFI IPv4,         10.0.0.4/30, tag 0x0000, metric: 1, next-hop: self
     AFI IPv4,        10.0.0.12/30, tag 0x0000, metric: 2, next-hop: self
     AFI IPv4,     192.168.1.0/24, tag 0x0000, metric: 1, next-hop: self
     AFI IPv4,     192.168.3.0/24, tag 0x0000, metric: 2, next-hop: self
   0x0000:  0202 0000 0002 0000 0a00 0004 ffff fffc
   0x0010:  0000 0000 0000 0001 0002 0000 0a00 000c
   0x0020:  ffff fffc 0000 0000 0000 0002 0002 0000
   0x0030:  c0a8 0100 ffff ff00 0000 0000 0000 0001
   0x0040:  0002 0000 c0a8 0300 ffff ff00 0000 0000
   0x0050:  0000 0002
```

Questions :

a. À quoi sert l'adresse « `224.0.0.9` » et à quoi correspond la valeur « `520` » ?

b. Que peut-on apprendre sur les interfaces du routeur qui a envoyé ce paquet ?