Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Infrastructure Réseau

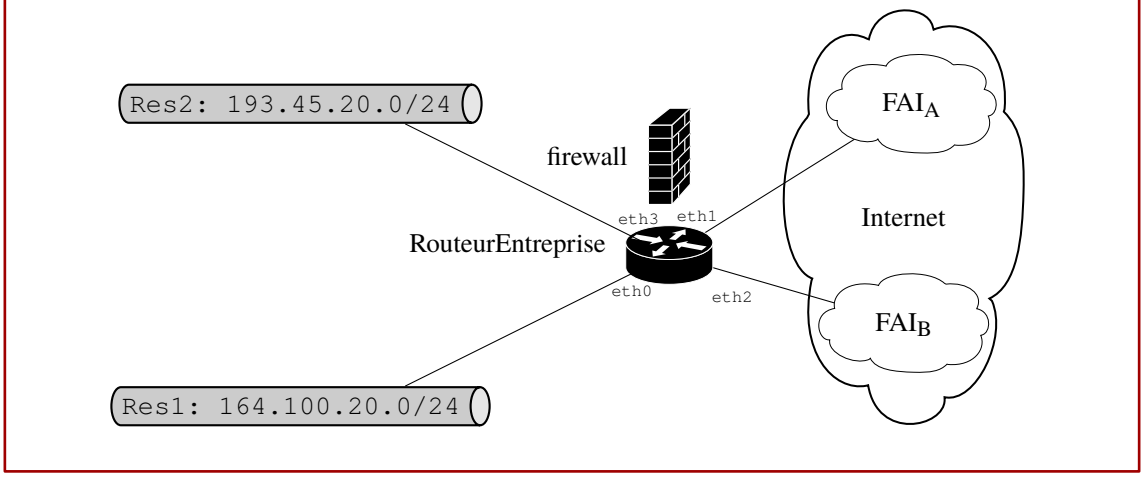
Corrections TD n°3

Routage, « Policy-based Routing » et BGP

1 – Un réseau dispose de l'adresse `193.50.185.0/24`.
Expliquez comment, un **serveur de fichier connecté dans ce réseau** peut communiquer avec deux sous-ensembles de machines de ce réseaux suivant deux adresses d'origine différentes à l'aide de la notion de scope.
Il faut découper le réseau en deux scopes différents et pour chacun de ces scopes, utiliser une adresse source différente pour la configuration de l'interface du serveur.
L'adresse du réseau intial étant en `/24`, on va utiliser deux scopes en `/25`.
Vous donnerez :

- ☐ les deux adresses à utiliser pour configurer le serveur ;
  L'adresse réseau initiale est `193.50.185.0/24`
  Les deux adresses à utiliser pour le serveur sont :
  - ▷ *`193.50.185.128/25`;*
  - ▷ *`193.50.185.1/25`;*
- ☐ les plages d'adresses des deux sous-ensembles de machines atteignables par chaque adresse.
  - ◇ *la plage d'adresse `193.50.185.2-193.50.185.127` aura une réponse avec l'adresse source `193.50.185.1`;*
  - ◇ *la plage d'adresse `193.50.185.129-193.50.185.254` aura une réponse avec l'adresse source `193.50.185.128`.*

2 – Soit le réseau de l'entreprise :



Soit la configuration obtenue de la part des deux FAIs :

RouteurEntreprise	adresse IP	routeur de sortie	FAI
eth1	193.50.18.84/24	193.50.18.254	A
eth2	131.25.48.23/24	131.25.48.254	B

Questions :

a. Donnez la configuration permettant aux machines :
   - ◇ de Res1 d'aller vers Internet par le FAI_A ;
   - ◇ de Res2 d'aller vers Internet par le FAI_B.

   Pour pouvoir désigner « Internet » comme destination, il faut utiliser la route par défaut.
   *Si l'on veut utiliser deux chemins pour aller vers Internet, il faut disposer de **deux routes par défaut** ⟹ soient **deux tables de routage différentes**.*
   Création de deux tables de routages dans `/etc/iproute2/rt_tables.d/netlab.conf`:

versFAIA :

```
xterm
ip route add default via 193.50.18.254
table versFAIA
```

versFAIB :

```
xterm
ip route add default via
131.25.48.254 table versFAIB
```

Puis on configure les « règles *» qui permettent de les sélectionner :*

```
xterm
ip rule add from 164.100.20.0/24 lookup versFAIA
ip rule add from 193.45.20.0/24 lookup versFAIB
```

b. On veut que :
   - ◇ tout le trafic Web de Res1 et Res2 aille vers FAI_A ;
     On peut le faire avec « ip rule *» :*

     ```
     xterm
     sudo ip rule add ipproto tcp dport 80 lookup versFAIA
     sudo ip rule add ipproto tcp dport 443 lookup versFAIA
     ```

     Ou avec le firewall :

     ```
     xterm
     sudo iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
     sudo iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
     sudo ip rule add fwmark 1 lookup versFAIA
     ```

   - ◇ tout le trafic SSH de Res1 et Res2 aille vers FAI_B ;
     On peut le faire avec « ip rule *» :*

     ```
     xterm
     sudo ip rule add ipproto tcp dport 22 lookup versFAIB
     ```

     Ou avec le firewall :

     ```
     xterm
     sudo iptables -t mangle -A PREROUTING -p tcp --dport 22 -j MARK --set-mark 2
     sudo ip rule add fwmark 2 lookup versFAIB
     ```

     Pour influencer le routage, il faut que le firewall intervienne avant la décision de routage, c-à-d en « PREROUTING *».*

c. Est-il possible que pour un trafic quelconque en provenance d'un des FAI et à destination de Res1 ou Res2, le trafic de retour passe par le même FAI d'origine ?
Non, ce n'est pas possible directement.

Oui, c'est possible si l'adresse source des paquets entrant par un FAI est modifiée pour être « associée *» à ce FAI.*

Comment faire ?
⟹*chacune des interfaces du RouteurEntreprise vers Res1 et Res2 doit posséder deux adresses IP différentes :*
- ◇ *interface eth2 : @IP_PROVA_eth3 et @IP_PROVB_eth3 appartenant à Res2 ;*
- ◇ *interface eth0 : @IP_PROVA_eth0 et @IP_PROVB_eth0 appartenant à Res1 ;*

Il faut identifier le FAI d'origine pour le trafic en entrée du routeur :

```
xterm
sudo iptables -t mangle -A PREROUTING -i eth1 -j mark --set-mark 1
sudo iptables -t nat -A POSTROUTING -m mark --mark 1 -o eth3 -j SNAT --to
@IP_PROVA_eth3
sudo iptables -t nat -A POSTROUTING -m mark --mark 1 -o eth0 -j SNAT --to
@IP_PROVA_eth0
```

et :

```
xterm
sudo iptables -t mangle -A PREROUTING -i eth2 -j mark --set-mark 2
sudo iptables -t nat -A POSTROUTING -m mark --mark 2 -o eth3 -j SNAT --to
@IP_PROVB_eth3
sudo iptables -t nat -A POSTROUTING -m mark --mark 2 -o eth0 -j SNAT --to
@IP_PROVB_eth0
```

Ensuite, il faut marquer les paquets retour pour permettre leur sortie vers FAIA ou FAIB

```
xterm
sudo iptables -t mangle -A PREROUTING -s @IPPROVA_eth0 -j MARK --set-mark 3
sudo iptables -t mangle -A PREROUTING -s @IPPROVB_eth0 -j MARK --set-mark 4
sudo iptables -t mangle -A PREROUTING -s @IPPROVA_eth3 -j MARK --set-mark 3
sudo iptables -t mangle -A PREROUTING -s @IPPROVB_eth3 -j MARK --set-mark 4
```

Ce qui permet aux paquets retour d'aller vers le bon FAI :

xterm
```
sudo ip rule add fwmark 3 lookup versFAIA
sudo ip rule add fwmark 4 lookup versFAIA
```

Attention

Cette solution n'est pas recommandée dans la mesure où l'origine d'une communication est masquée par le SNAT pour les machines de Rés1 et de Rés2 ce qui peut entraîner des problèmes de sécurité.
Cette solution fonctionne aussi uniquement pour des protocoles avec suivi de « connexion *» dans le firewall.*
On utilisera plutôt des notions de « flow *» (couples TSAP/protocoles) dans le routeur basée sur les SDN, «* Software Defined network *».*

3 – Dans le cas d'une attaque au travers de BGP où une AS malveillante annonce un réseau qui ne lui appartient pas afin de détourner le trafic à sa destination, que peut faire l'AS légitime pour rediriger le trafic vers son réseau en utilisant des annonces BGP ?

Vous utiliserez les informations suivantes :
- ▷ le réseau annoncé par l'AS légitime 1935 est `164.81.56.0/26` ;
- ▷ l'AS menant l'attaque est l'AS1234.

Pour rediriger le trafic vers l'AS légitime, il faut distribuer une route plus « attractive *» que celle diffusée par l'AS menant l'attaque car définie pour un préfixe plus long que l'original.*
L'AS1234 menant l'attaque diffuse un chemin vers le réseau `164.81.56.0/26`, il faut donc diffuser des réseaux avec un préfixe plus long et couvrant l'intégralité des adresses du réseau initial :
Il faut donc diffuser les deux réseaux suivants :

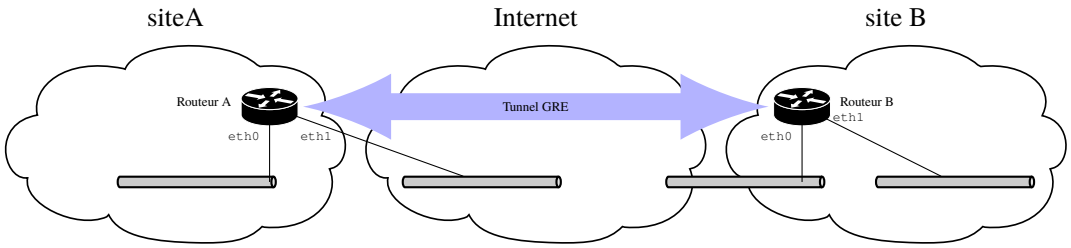
		/26	/27				
0	0	0	0	0	0	0	0
128	64	32	16	8	4	2	1

⟹*le réseau `164.81.56.0/27`*

		/26	/27				
0	0	0	0	1	0	0	0
128	64	32	16	8	4	2	1

⟹*le réseau `164.81.56.32/27`*

4 – Un tunnel GRE doit être mis en place entre deux routeurs du réseau de la même entreprise répartie entre deux sites distants.



La configuration est la suivante :

Routeur A

```
eth0     10.0.0.100/24
eth1     193.50.178.131/24
default  193.50.178.254
```

Routeur B

```
eth0     135.27.31.45/24
eth1     164.81.1.21/24
default  135.27.31.254
```

a. Donnez la configuration des deux routeurs pour l'accès à Internet (Routage/Firewall).
Le RouteurA est connecté à un réseau privé sur eth0 ⟹faire du SNAT pour autoriser le trafic à aller sur Internet.
Routeur A :

Destination	*next hop*
10.0.0.0/24	*10.0.0.100*
193.50.178.0/24	*193.50.178.131*
default	*193.50.178.254*

Routeur B :

Destination	*next hop*
135.27.31.0/24	*135.27.31.45*
164.81.1.0/24	*164.81.1.21*
default	*135.27.31.254*

xterm
```
sudo iptables -t nat -A POSTROUTING -s
10.0.0.0/4 -o eth1 -j MASQUERADE
```

b. Donnez la configuration de « RouteurA » et « RouteurB » pour mettre en place un tunnel GRE permettant de lier les deux sites A et B.

Sur RouteurA :

```
xterm
sudo ip tunnel add mon_tunnela mode gre local 193.50.178.131 remote 135.27.31.45
sudo ip address add 172.16.0.1/24 dev mon_tunnela
sudo ip link set mon_tunnela up
```

Sur RouteurB :

```
xterm
sudo ip tunnel add mon_tunnelrb mode gre local 135.27.31.45 remote
193.50.178.131
sudo ip address add 172.16.0.2/24 dev mon_tunnelb
sudo ip link set mon_tunnelb up
```

c. On veut que :

- pour des raisons de confidentialité, tout le trafic Web non sécurisé vers le port 80 passe par le tunnel mis en place pour circuler entre les deux sites ;
- et celui sécurisé vers le port 443 n'emprunte pas le tunnel pour circuler entre les deux sites.

Donnez la configuration du firewall/routage pour permettre ce comportement.
Sachant que ce sont les protocoles et non pas les adresses de destination qui force le passage dans le tunnel, il faut changer la vision du routage depuis le SiteA vers le SiteB :

- *une vision passant par Internet*
- *une vision passant par le tunnel ;*

⟹ *il faut deux tables de routage : celle normale et une utilisant le tunnel.*

Sur RouteurB, le réseau du SiteA étant privé, il n'y a pas d'autres moyens que de passer par le tunnel pour l'atteindre.
⟹ *il suffit d'ajouter une destination dans la table de routage.*

Sur RouteurA, on ajoute la table de routage `par_tunnel` *:*

Destination	*nex hop*
164.81.1.0/24	*172.16.0.2*

Sur RouteurB, on ajoute dans la table de routage existante :

Destination	*next hop*
135.27.31.0/24	*135.27.31.45*
164.81.1.0/24	*164.81.1.21*
10.0.0.0/24	*172.16.0.2*
default	*135.27.31.254*

la règle de firewall suivante :

```
xterm
sudo iptables -t mangle -A PREROUTING -p
tcp --dport 80 -j MARK --set-mark 1
```

et la règle de routage suivante :

```
xterm
sudo ip rule add fwmark 1 lookup
par_tunnel
```

Pour la configuration du firewall sur RouteurA, on pourra ajouter la sécurité de la gestion des états de connexion fournie par le module « state *».*
Ici, on estime que le trafic passant par le tunnel est considéré comme « interne *» à l'entreprise.*

Attention

Un tunnel GRE ne protège pas le contenu du trafic qu'il transporte : il n'y a pas de ***chiffrement****.*

d. Comment améliorer la QoS des datagrammes GRE ?
On peut faire :

- *du «* traffic shaping *» pour privilègier la sortie des paquets du tunnel sur les routeurs A et B par rapport aux autres paquets ;*
- *du positionnement du TOS en espérant que le réseau Internet en tienne compte et que le routeur en face privilégie leur entrée par rapport aux autres paquets.*