Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

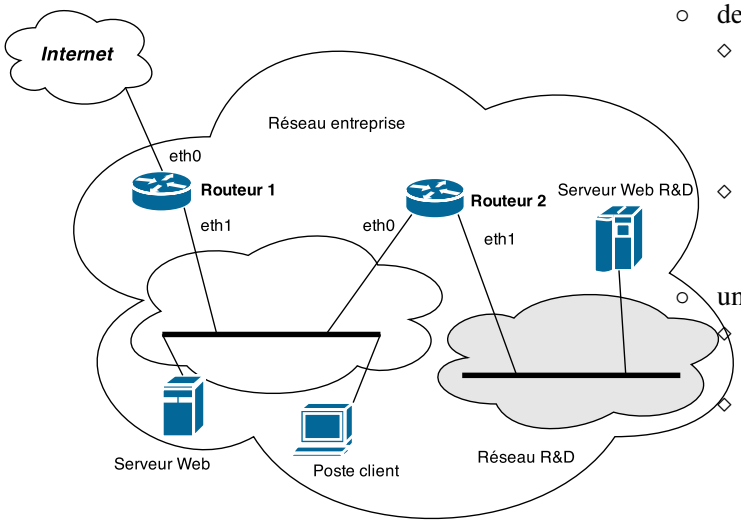
Réseaux Avancés I

Examen — janvier 2014

Durée : 2h — Documents autorisés

NetFilter — (6 points)

1 – 6pts Le responsable du système d'information d'une entreprise fait appel à vous pour mettre en place une politique de sécurité dans le réseau dont le synoptique est indiqué ci-dessous :



- deux routeurs sous Linux avec NetFilter :
  - « Routeur 1 » :
    - « `eth0` » : `118.23.37.41/18`, route par défaut `118.23.37.54` ;
    - « `eth1` » `192.168.255.254` ;
  - « Routeur 2 » :
    - « `eth0` » : `192.168.254.253` ;
    - « `eth1` » ;
- un réseau organisé en deux zones :
  - zone « à accès normal », où se trouve la machine « Poste client » ;
  - zone « à accès restreint », où se trouve la machine « Serveur R&D » :

La **politique de sécurité** est la suivante :

I. la « policy » utilisée par NetFilter doit être « DROP » par défaut ;

II. le réseau de l'entreprise utilise une adresse réseau de type privée : `192.168.0.0/16` ;

III. les machines connectées dans la zone « à accès normal », comme « Poste client » :
   - ne doivent pas connaitre l'existence de la zone grise, c-à-d le « Réseau R&D » : elles seront configurées pour voir le réseau en `192.168.0.0/16` ;
   - doivent pouvoir accéder à Internet ;

IV. les machines de la zone « Réseau R&D » doivent :
   - avoir le droit d'accèder au « Serveur Web » dans la zone « à accès normal » (celle contenant la machine « Poste Client ») ;
   - avoir le droit d'accèder à Internet ;

V. seule la machine « Poste Client » configurée en `192.168.1.1` a le droit de se connecter au « Serveur Web R&D » ;

Questions :

a. Vous donnerez la configuration de routage des routeurs « Routeur 1 » et « Routeur 2 », ainsi que la configuration de la machine « Poste Client ».

b. Vous donnerez la configuration des firewalls NetFilter de « Routeur 1 » et « Routeur 2 » mettant en œuvre la politique de sécurité décrite.
Vous indiquerez sur vos règles de firewall à quelle règle de la politique de sécurité elle est associée (règle I à V).

c. Est-il possible de :
   - permettre l'accés depuis Internet au « Serveur Web R&D » ?
   - de masquer le passage par le routeur « Routeur 2 » à un observateur extérieur ?

Vous donnerez les règles de firewall à ajouter à la configuration précédente.

TCP & QoS — (8 points)

2 – 2pts Soit la configuration TCP des machines suivantes :

Machine	Taille fenêtre Réception
A	10000
B	20000

Calculez le débit maximal de la communication de A $\longrightarrow$ B sachant que le RTT entre A et B est de 2sec.

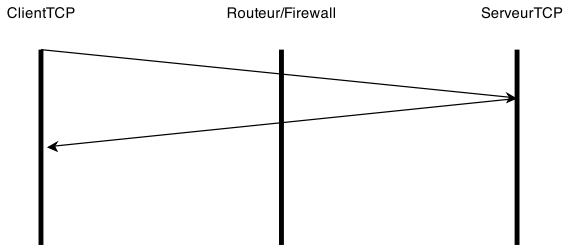
3 – 3pts Un administrateur désirant réaliser de la QoS sur une connexion TCP à destination de la machine ServeurTCP `164.81.90.17` appartenant au réseau qu'il administre vient d'intégrer la règle suivante dans la configuration du firewall NetFilter :

```
iptables -t filter -A FORWARD -p tcp --dport 899 -m limit --limit 20/min --limit-burst 1
  -j ACCEPT
```

La machine ClientTCP va se connecter depuis l'extérieur du réseau vers la machine ServeurTCP et le RTT observé entre ClientWeb et ServeurTCP est de 3sec (le temp d'acheminement entre le Routeur/firewall et ServeurTCP est négligeable).

Décrivez comment va se comporter les échanges TCP sachant que :

- ▷ la machine ClientTCP utilise l'algorithme Tahoe ;
- ▷ le protocole de niveau 5 envoie beaucoup de données du client vers le serveur en début de connexion (au moins plus d'une centaine de segments de taille MSS) ;
- ▷ le RTO est de 6sec sur la machine ClientTCP ;
- ▷ la machine ServeurTCP dispose d'une fenêtre de réception de taille supérieure à $20 * MSS$;



Vous indiquerez l'évolution de la fenêtre de congestion, les segments envoyés, perdus, retransmis *etc.* pour les 10 premières secondes de la connexion.

4 – 3pts Comparaison des VLANs et de la technologie MPLS

Vous énumérez des ressemblances et des différences en terme de :

a. intégration dans la couche de niveau 2 ;

b. intéraction avec la couche de niveau 3 ;

c. sécurité des échanges ;

d. QoS des échanges ;

e. mise en œuvre dans le réseau d'une entreprise ;

f. admnistration.

Programmation — (6 points)

ATTENTION

Deux exercices sont proposés en fonction de votre parcours CRYPTIS ou ISICG.
Vous avez le droit de choisir l'exercice que vous voulez parmi les deux proposés.

5 – 6pts Pour illuster un exemple dans le cadre de la rédaction d'un livre d'apprentissage de la programmation Web combinant AngularJS, Bottle, JQuery et JSON, on veut créer l'exercice suivant :

I. une application Python utilisant Bottle fournie une page HTML au navigateur de l'utilisateur ;
II. un compteur est affiché sur la page HTML du navigateur de l'utilisateur ;
III. un bouton est affiché à côté :
   - ◇ lors de l'appui sur le bouton, une requête est transmise à l'application Python ;
   - ◇ une variable Python est incrémentée ;
   - ◇ la valeur incrémentée de cette variable est renvoyée au navigateur de l'utilisateur ;
   - ◇ le compteur affiché dans le navigateur de l'utilisateur est mis à jour avec la nouvelle valeur ;

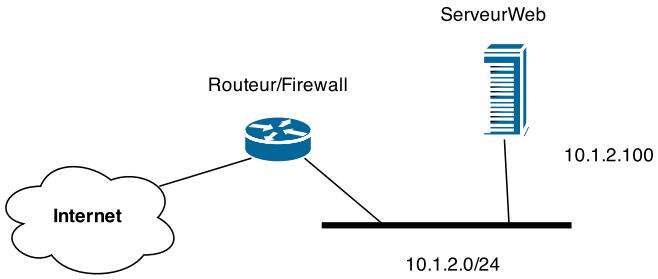
IV. un **seul utilisateur à la fois** est concerné par la gestion de ce compteur ;

Questions :

a. Vous fournirez le code Python de l'application Bottle, de la page HTML et du code Javascript réalisant l'échange entre le navigateur et l'application.

b. Si on voulez permettre la gestion entre diférents utilisateurs simultanément de ce compteur, quelle technologie faudrait-il utiliser ?
Vous justifierez briévement votre réponse.

6 – 6pts On voudrait permettre à une machine hébergeant un serveur Web de contrôler le firewall s'exécutant sur le routeur qui la sépare du réseau Internet :



La machine ServeurWeb doit être capable avec un **logiciel Python client** de changer les règles du firewall afin de :

- ⋆ autoriser les connexions Web depuis Internet vers elle-même sur le port 80 et pour le protocole TCP ;
- ⋆ enlever cette autorisation.

Questions :

a. Quel protocole de transport allez vous utiliser pour mettre en œuvre ce protocole de reconfiguration du firewall ?
Comment vont être exprimés les ordres du logiciel client ?

b. Vous donnerez le code du programme Python réalisant le travail du Serveur localisé sur le Routeur/Firewall en accord avec votre proposition précédente :
   - ◇ réception des ordres d'autorisation/limitation de la part du ServeurWeb ;
   - ◇ reconfiguration du firewall.