

<b>Institut National des Télécommunications</b>	<b>Module : ISSR34 - Filtrage</b>	
Domaine: <b>Sécurité - 3<sup>ème</sup> Année.</b>	Responsable : Olivier Paul	
Durée: <b>2H00</b>	Documents : <b>Autorisés</b>	Nombre de pages : <b>5 pages</b>
<b>NOM :</b>	<b>Prénom :</b>	<b>Note:</b>

- L'épreuve comporte deux exercices.
- Le document est accompagné de trois annexes:
  - Annexe 1: Article «Securing your network against Kazaa» de 7 pages.
  - Annexe 2: trace d'une communication ssh obtenue avec ethereal.
  - Annexe 3: trace d'une communication ssh.

**Exercice I : Filtrage et Kazaa**

(14 points)

Lisez l'article en annexe 1 avant de répondre aux questions suivantes.

**I.1** Peut on filtrer le protocole FastTrack en utilisant des règles de filtrage statiques de niveau réseau ?, Expliquez.

**I.2** Peut on filtrer le protocole FastTrack en utilisant la combinaison d'un proxy http et de règles de filtrage statiques de niveau réseau ?, Expliquez.

**I.3.** Pourquoi l'auteur ne choisit il pas cette solution, Quels problèmes peut elle poser ?

**I.4.** Comment firewall se positionne t il en terme de couche protocolaire (réseau, circuit, application) ? Comment se positionne t il en terme d'implantation (noyau, espace utilisateur) ? Dessinez schématiquement la relation entre les différents éléments permettant jouant un rôle dans l'architecture de filtrage.

**I.5.** Cette architecture peut elle poser de problèmes pour les utilisateurs qui n'utilisent pas de logiciel P2P ? Pourquoi ?

**I.6.** Quelles sont les différentes phases permettant de s'assurer que le protocole FastTrack ne passe pas le pare-feux ?

I.7. Ces phases peuvent elles poser des problèmes pour les utilisateurs utilisent un logiciel P2P ? Pourquoi ?

I.8. Comment sont contrôlées les communications de l'extérieur vers l'intérieur ?

L'auteur mentionne en début d'article l'utilisation d'un module `ip_string` qui permet de rechercher des motifs particuliers (chaînes de caractère) dans les données des paquets IP dans le module de filtrage du noyau.

I.9. A quoi selon vous une telle extension peut elle servir ?

## Exercice II : SSH et NAT

(6 points)

Une entreprise possède un réseau connecté au réseau Internet. L'adresse du réseau fourni à celui-ci est le 193.168.123.0/30. L'entreprise souhaite permettre à des collaborateurs distants de se connecter sur des équipements internes au travers de deux serveurs SSH. Le préfixe fourni à l'entreprise étant très petit, il est décidé d'utiliser un NAT statique entre le réseau externe et le réseau de l'entreprise. On attribue alors aux

serveurs SSH les adresses 192.168.0.2 et 192.168.0.3. On donne par ailleurs comme adresse au NAT l'adresse 193.168.123.1.

**II.1** Dessinez un diagramme dans lequel vous positionnerez les équipements et leurs adresses.



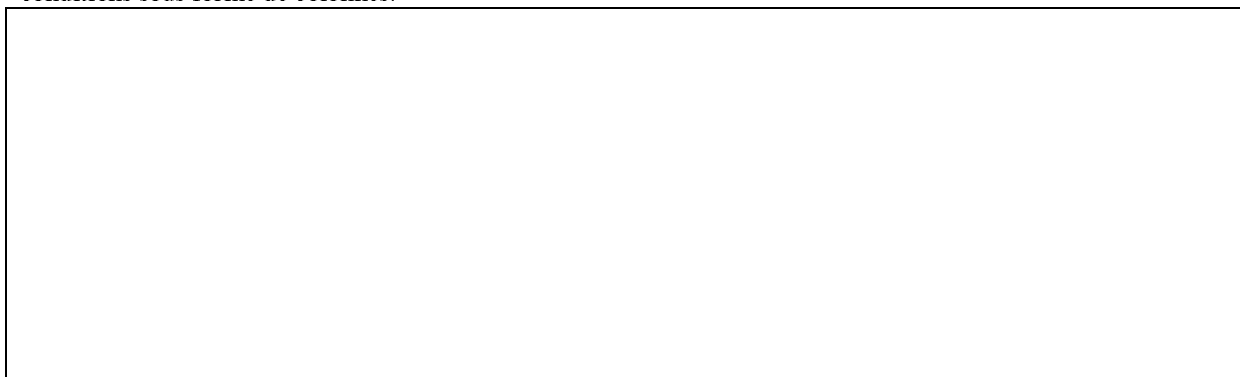
On rappelle que le port associé à SSH est le port 22.

**II.2** Donnez les règles donnant les relations entre adresses/ports publics adresses/ports privés.

Adresse Src	Port Src	Adresse Dest.	Port Dest.

Notre NAT a en plus la capacité de réaliser du filtrage de niveau réseau. On désire maintenant configurer ce filtrage afin de limiter les accès externes au NAT. Pour cela on se place entre le NAT et le réseau interne et on réalise une communication avec le serveur SSH depuis l'extérieur que l'on capture avec un analyseur de trafic. Le résultat est donné en annexe 2.

**II.3** Donnez les règles de filtrage de niveau réseau pour les interfaces internes et externe. On suppose que le filtrage est réalisé après l'opération de traduction d'adresse. Afin de faciliter la lecture on ordonnera les conditions sous forme de colonnes.





On désire maintenant tester le second serveur SSH sur la machine d'adresse 192.168.0.3. Pour cela on se connecte sur cet équipement depuis un équipement extérieur. L'annexe 3 représente la capture de l'écran de connexion.

**II.4** Qu'en concluez vous concernant le protocole SSH ? Expliquez.

