

Institut National des Télécommunications	Module : ISSR14 - Filtrage	
Domaine: Sécurité - 3^{ème} Année.	Responsable : Olivier Paul	
Durée: 2H30	Documents : Interdits	Nombre de pages : 8 pages
NOM :	Prénom :	Note:

- L'épreuve comporte deux exercices.
- Le document est accompagné de quatre annexes:
 - Annexe 1: trace d'une communication ftp obtenue avec ethereal.
 - Annexe 2: trace d'une communication ftp obtenue avec ethereal.
 - Annexe 3: trace d'une communication ftp obtenue avec ethereal.
 - Annexe 4 Le RFC 959 spécifiant le protocole FTP, la lecture complète de ce document n'est pas nécessaire pour réaliser l'épreuve. Ce document sert juste de référence pour répondre à certaines questions. **La lecture préalable du document RFC 959 est fortement déconseillée.**

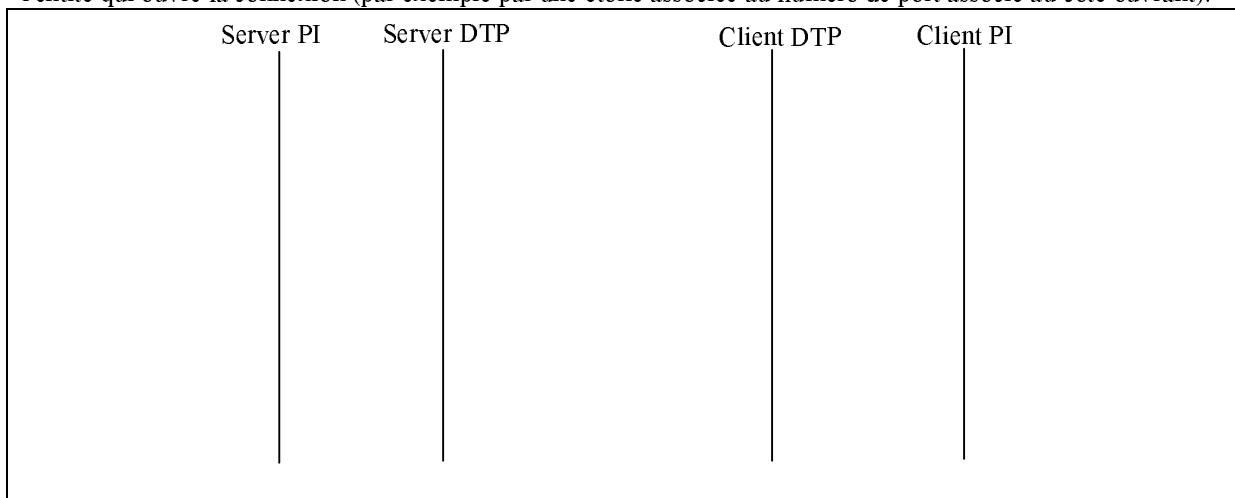
Exercice I : FTP et Filtrage (12 points)

Une entreprise possède deux sites interconnectés par le réseau Internet. Le site A possède l'adresse réseau 193.168.123.128/25. Le site B possède l'adresse réseau 193.168.123.0/25. On désire fournir un service d'échange de fichiers entre les deux sites. Pour cela on place un serveur ftp sur un serveur d'adresse IP 193.168.123.129 en A. Pour restreindre les communications on dispose de routeurs filtrants.

I.1 Réalisez un diagramme du réseau dans lequel vous positionnerez des équipements de filtrage.

Afin de nous aider à définir la politique de contrôle d'accès entre les deux équipements, on réalise une communication entre un client ftp localisé sur un équipement du site B et le serveur ftp du site A sans filtrage. La trace de cette communication est donnée en annexe 1.

I.2 Sur un diagramme temporel, indiquez les interactions entre entités protocolaires **FTP** telles que décrites dans le RFC 959 (section 2.3 page 9). On utilisera les communications TCP pour définir les numéros de port utilisés de part et d'autre. On indiquera le numéro de du paquet associé à chaque échange. . Pour chaque connexion l'entité qui ouvre la connexion (par exemple par une étoile associée au numéro de port associé au coté ouvrant).



--	--	--	--	--

1.3 Définissez les politiques de contrôle d'accès en terme de protocoles (proto), d'adresses et de masques (SrcIP, DstIP, /x), de numéros ports source et destination (SrcPort, DstPort), de direction (Dir) et d'action (Action) pour faire en sorte que cette communication puisse se dérouler de manière correcte.
On simplifiera les règles en supposant que l'on ne considère que l'interface externe de chaque filtre (symétrie entre interfaces).

--

I.4 A quoi sert la commande PORT (RFC 959 section 4.1.2) ? Quels sont les risques associés à ces règles? Un client FTP peut il être perturbé ? Comment ?

On s'intéresse par la suite au problème de perturbation des clients FTP situés en B.

I.5 Supposons que l'on puisse spécifier en complément des paramètres de filtrage précédents la valeur des drapeaux TCP (TCPf). On supposera que l'on pourra spécifier la valeur SYN pour un paquets représentant une demande d'ouverture de connexion. Définissez les politiques de contrôle d'accès en terme de protocoles (proto), d'adresses et de masques (SrcIP, DstIP, /x), de numéros ports source et destination (SrcPort, DstPort), de direction (Dir) pour faire en sorte que cette communication puisse se dérouler de manière correcte.

On simplifiera les règles en supposant que l'on ne considère que l'interface externe de chaque filtre (symétrie entre interfaces).

I.6 Le problème de perturbation du client FTP est il résolu ?

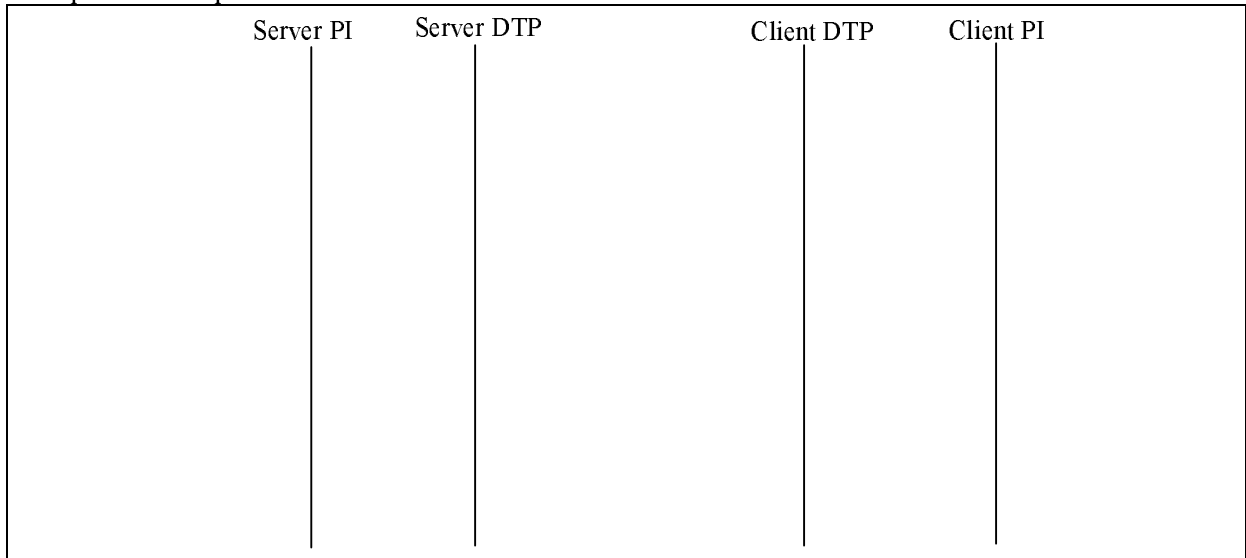
I.6 Supposons que l'on puisse associer au niveau de chaque filtre un état à chacune des connexions. On utilise cet état pour faire en sorte qu'un paquet n'est accepté par le filtre que si son numéro de séquence est correct vis à vis de la fenêtre TCP du récepteur de la connexion. On supposera que les numéros de séquence TCP sont choisis de manière suffisamment sûre pour que des attaquants ne puissent les deviner. Quels risques permet de supprimer cette évolution ? Le problème de perturbation du client FTP est-il résolu ?

On étudie maintenant une commande du protocole ftp appelée ouverture passive (PASV)

I.7 Décrivez la fonction de cette commande.

Afin de construire une politique de contrôle d'accès prenant en compte cette commande on réalise une communication entre un client ftp localisé sur un équipement du site B et le serveur ftp du site A sans filtrage. On étudie les différences entre la trace produite par l'utilisation de la commande PASV et la trace précédemment produite. Cette trace est fournie en annexe 2.

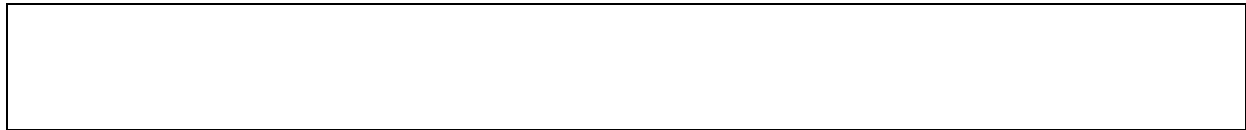
I.8 Sur un diagramme temporel, indiquez les interactions entre entités protocolaires **FTP** telles que décrites dans le RFC 959 (section 2.3 page 9). On utilisera les communications TCP pour définir les numéros de port utilisés de part et d'autre. On indiquera le numéro de du paquet associé à chaque échange. Pour chaque connexion on indiquera l'entité qui ouvre la connexion.



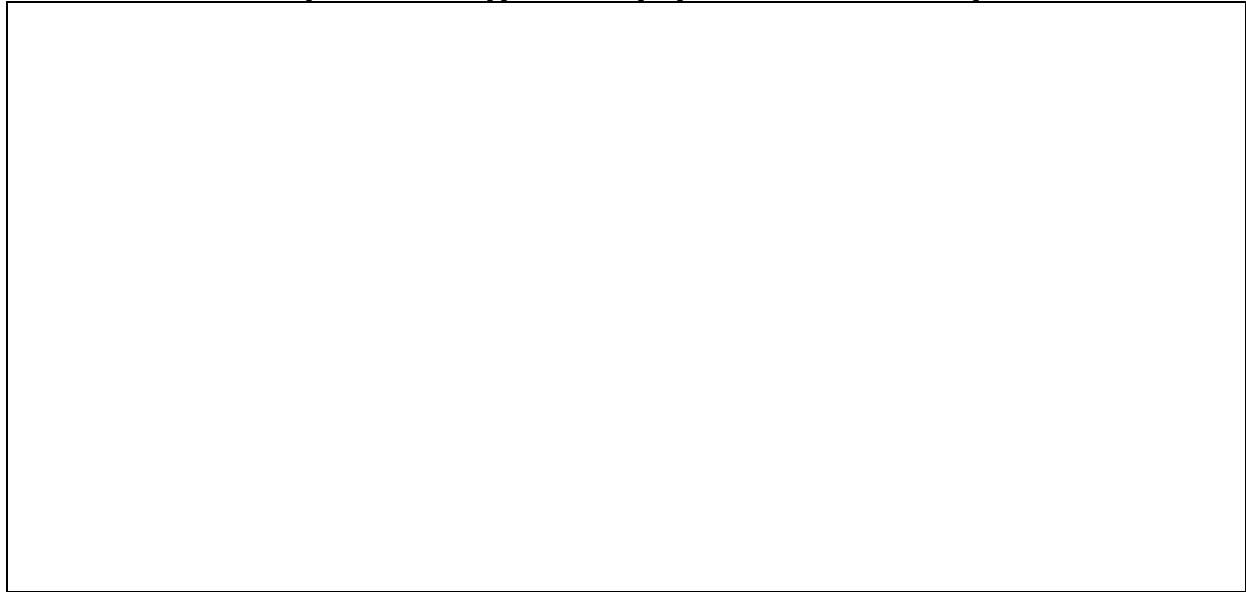
--	--	--	--	--

I.9 On supposera que l'on pourra spécifier la valeur SYN pour les paquets représentant une demande d'ouverture de connexion. Définissez les politiques de contrôle d'accès en terme de protocoles (proto), d'adresses et de masques (SrcIP, DstIP, /x), de numéros ports source et destination (SrcPort, DstPort), de direction (Dir) et de drapeaux TCP (TCPf) pour faire en sorte que cette communication puisse se dérouler de manière correcte. On simplifiera les règles en supposant que l'on ne considère que l'interface externe de chaque filtre (symétrie entre interfaces).
On supposera que l'on réalise un filtrage à état comme spécifié précédemment.

--



I.10 La commande PASV permet elle de supprimer le risque pour les clients FTP ? Pourquoi ?



Exercice II : FTP et NAT

(8 points)

Une entreprise possède deux sites interconnectés par le réseau Internet. Le site A possède l'adresse réseau 193.168.123.0/29. Le site B possède l'adresse réseau 193.168.123.8/29. On utilise par ailleurs un domaine d'adressage privé 192.168.123.1/25 dans chacun des sites (les deux domaines utilisent donc la même plage d'adresse privée). On désire fournir un service d'échange de fichiers entre les deux sites. Pour cela on place un serveur ftp sur un serveur d'adresse IP 193.168.123.2 en A. Afin que les utilisateurs puissent accéder au serveur de manière simultanée, on utilise un NAT avec traduction de port (NATPT). Conformément au RFC 2663 un NATPT est définit par:

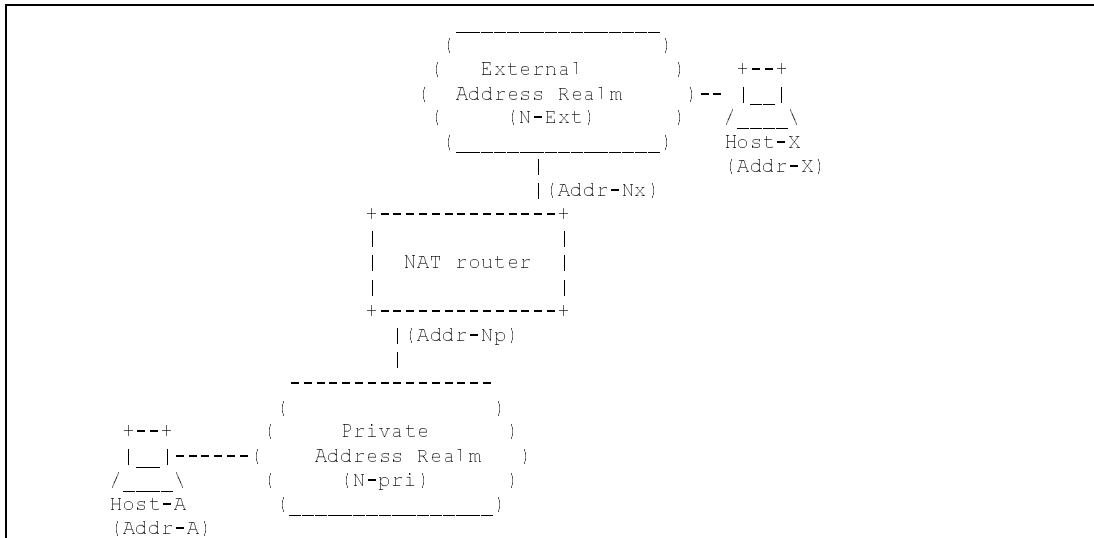


Figure 2: A base model to illustrate NAT terms.

4.1.2. Network Address Port Translation (NAPT)

NAPT extends the notion of translation one step further by also translating transport identifier (e.g., TCP and UDP port numbers,

ICMP query identifiers). This allows the transport identifiers of a number of private hosts to be multiplexed into the transport identifiers of a single external address. NAT allows a set of hosts to share a single external address. Note that NAT can be combined with Basic NAT so that a pool of external addresses are used in conjunction with port translation.

For packets outbound from the private network, NAT would translate the source IP address, source transport identifier and related fields such as IP, TCP, UDP and ICMP header checksums. Transport identifier can be one of TCP/UDP port or ICMP query ID. For inbound packets, the destination IP address, destination transport identifier and the IP and transport header checksums are translated.

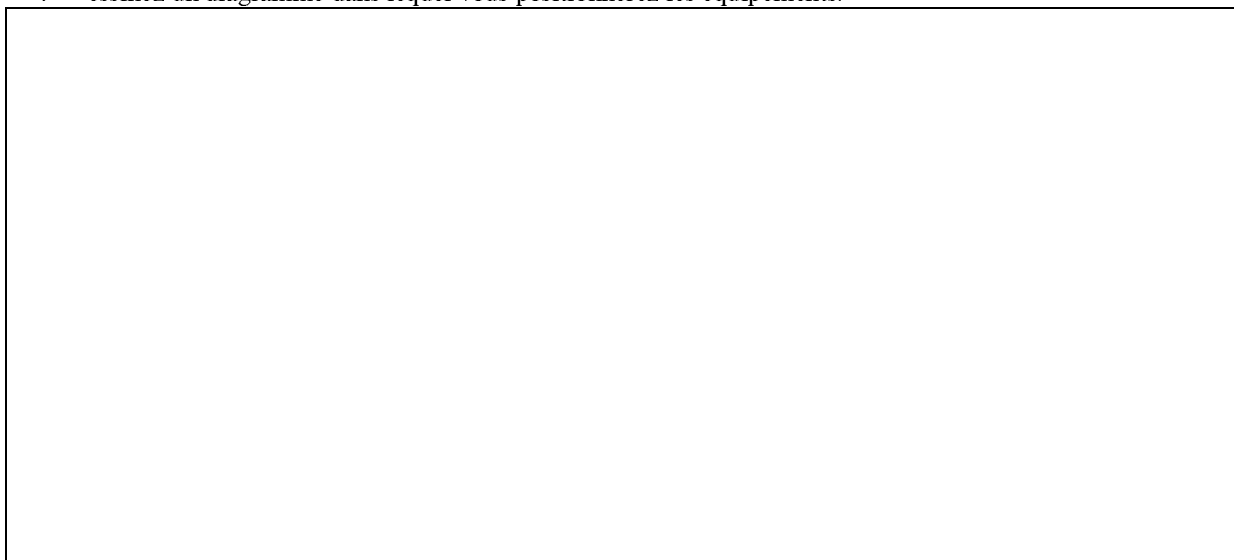
A NAT router in figure 2 may be configured to translate sessions originated from N-Pri into a single external address, say Addr-i.

Very often, the external interface address Addr-Nx of NAT router is used as the address to map N-Pri to.

On attribue au NAT en A l'adresse IP externe 193.168.123.3. On attribue au NAT en B l'adresse IP externe 193.168.123.9.

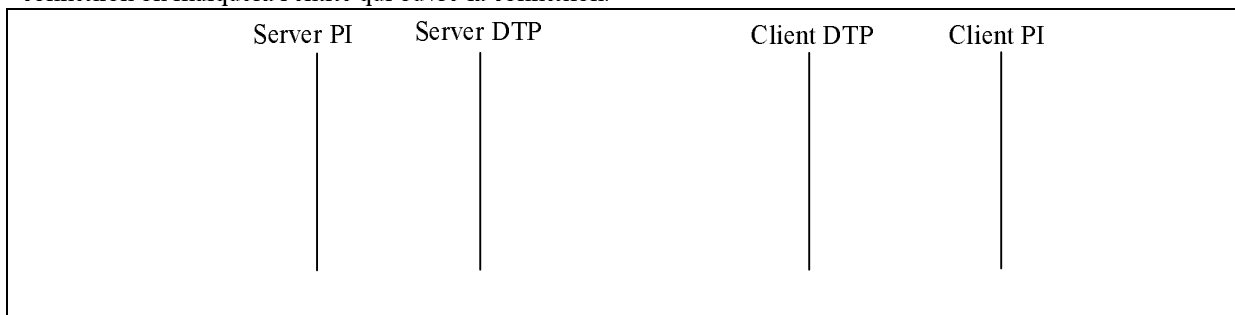
On désire par ailleurs que les utilisateurs des deux sites ne puissent accéder qu'à ce service. Pour restreindre les communications on dispose de routeurs filtrants.

II.1 Dessinez un diagramme dans lequel vous positionnerez les équipements.



Afin de construire une politique de contrôle d'accès prenant en compte cette commande on réalise une communication entre un client ftp localisé sur un équipement du site B et le serveur ftp du site A sans filtrage. On étudie la trace produite par cette communication au moyen d'un analyseur positionné sur le site A entre l'équipement NAT et le routeur filtrant. Cette trace est fournie en annexe 3.

II.2 Sur un diagramme temporel, indiquez les interactions entre entités protocolaires **FTP** telles que décrites dans le RFC 959 (section 2.3 page 9). On utilisera les communications TCP pour définir les numéros de port utilisés de part et d'autre. On indiquera le numéro de du paquet associé à chaque échange. Pour chaque connexion on indiquera l'entité qui ouvre la connexion.



--	--	--	--	--

II.3 Quel est le problème engendré par la présence du NAT ?

--

II.4 Que proposeriez vous pour résoudre ce problème ?

--