Règles de Filtrage d'un Pare-Feu

TD 6 Réseaux — Module TR2 — R&T2A

20 octobre 2008

Exercice 1 : On considère le réseau de l'ENSIL dont l'architecture est décrite en **Annexe** 1 et **Annexe** 2. Le fonctionnement de cette architecture est caractérisé par les points suivants :

- L'organisation logique du réseau de l'ENSIL s'articule sur 5 VLANs répartis de la façon suivante :

Nom du réseau	VLAN Id	Adresse IP du réseau
Serveurs	1	193.49.176.0/24
Administration	2	192.168.4.0/24
PC Profs	3	192.168.9.0/24
WIFI	4	192.168.8.0/24
PC Etudiants	5	192.168.7.0/24

- Sur le commutateur OptiSwitch 800 est connecté un Routeur **Netasq F500**. Le Netasq F500 est désigné par le constructeur comme un Firewall. Il est configuré de façon à intégrer les fonctions suivantes : firewall, routeur et serveur DHCP.
- La communication directe entre les différents réseaux de l'ENSIL n'est possible qu'à travers le Netasq. Ce dernier assure le routage "InterVlan(s)". Sur son lien physique avec l'OptiSwitch, il possède donc une adresse IP par VLAN ; ses adresses sont indiquées par le tableau ci-dessous :

VLAN Id	Adresse IP du Netasq
1	193.49.176.250/24
2	192.168.4.254/24
3	192.168.9.254/24
4	192.168.8.254/24
5	192.168.7.254/24

- Le serveur proxy (réseau "Serveurs") assure uniquement les accès Web et FTP des stations de l'ENSIL, sauf pour toutes les stations du réseau "PC Profs" pour lesquelles le Netasq réalise alors une translation d'adresse IP. Les accès autres que Web et FTP se font sans passer par le proxy.
- Le Firewall/Bridge assure le filtrage du trafic entre le réseau externe, la DMZ et le réseau local ENSIL.
- Toutes les requêtes provenant du réseau externe sont dirigées vers les services de la DMZ.

– Seul le routeur Netasq et le serveur Proxy peuvent faire des requêtes vers l'extérieur.

– Dans le VLAN 4, la première adresse du réseau IP (soit 192.168.8.1/24) est attribuée au poste de supervision. Ce poste permet d'assurer la télémaintenance sur tous les postes et serveurs du site ENSIL.

Le firewall Netasq F500, en plus de la translation d'adresses IP et du foncrionnement décrit précedemment, a pour tâche **de filtrer le trafic entrant et sortant** en fonction du cahier des charges donné ci-dessous. Ce cahier des charges du Firewall est constitué des règles suivantes :

a) **Les accès WEB et FTP** :
Tous les accès directs Web et FTP vers Internet sont interdits sauf :

(a) requêtes et réponses pour les adresses IP du réseau "PC Profs" ;

(b) requêtes et réponses pour la station de Supervision ;

(c) les réponses du Proxy (port : 1080) sont autorisées vers le LAN.

b) **Les accès DNS** :
Seule la résolution DNS à destination du serveur "DNS Externe" situé dans la DMZ est autorisée.

Questions :

1. Donner la signification de DMZ. Dans quel cas utilise-t-on une DMZ ?
2. En vous basant sur ce cachier des charges et sur le document **Annexe** 3, écrire les règles de filtrage correspondantes en complétant le modèle de table ci-dessous :

SOURCE	PORT	DESTINATION	PORT	PROTOCOLE	ACTION (`permit`, `deny`)

– dans le cas ou la source et/ou la destination et/ou le port peuvent être indifférents, la (ou les) valeur(s) sera (seront) *Any*,
– la source ou la destination doit être spécifiée sous le format CIDR (*@IP/mask*),
– si la source ou la destination est un réseau, le masque sera celui du sous-réseau,
– si la source ou la destinationest un hôte, le masque sera /32.

3. Admettant que le Firewall laisse passer les requêqutes provenant d'Internet, est-il nécessaire de prévoir des règles qui protègent le LAN de ces accès ? Justifier votre réponse.