Auteur: P. Petit	*Titre: TD ASRA: introduction à l'utilisation de pf*	*Version: 1.0*
Date: 27/03/2006	Licence: Gnu Free Documentation Licence	Durée: 3h00

Elements de correction

Exercice 2: étude de règles classiques

1. expliquer les règles packet filter suivantes :

groupe de règles No 1:
 # par défaut, on bloque tout
bloc in all
bloc out all
 # on autorise le trafic de 192.168.0.0/24 vers l'hôte 192.168.1.1
 # comme on ne prévoit rien pour les paquets retour, ça ne sert pas à grand chose
pass in on dc0 from 192.168.0.0/24 to 192.168.1.1
groupe de règles No 2:
#idem groupe 1 mais là, on prévoit une autorisation pour les paquets retour
 # donc tout est autorisé entre le sous-réseau et l'hôte.
bloc in all
bloc out all
pass in on dc0 from 192.168.0.0/24 to 192.168.1.1
pass out on dc0 from 192.168.1.1 to 192.168.0.0/24
groupe de règles No 3:
 # on autorise tout du sous-réseau vers l'hôte et on active le suivi de connexions
 # ce qui permet aux paquets retour de passer. Donc toute connexion dont le premier paquet
 # vient du sous-réseau aura tous ses paquets autorisés.
 # par contre, les connexions depuis l'hôte vers le sous-réseau ne sont pas autorisées
bloc in all
bloc out all
pass in on dc0 from 192.168.0.0/24 to 192.168.1.1 keep state
groupe de règles No 4:
#des macros
my_ip="192.168.10.6"
if_in="dc0"
if_out="fxp0"
local_net="192.168.0.0/24"
#règles par défaut: on bloque tout
bloc in all
block out all
#on bloque depuis le réseau local vers 192.168.10.6 sans lire la suite des règles (quick)
block in quick from $local_net to $my_ip
#**on autorise ssh des hôtes du sous-réseau vers le reste du monde**
pass in on $if_in from $local_net proto tcp flags S/SA to any port ssh keep state
#**on autorise le dns tant en tcp qu'en udp du sous-réseau vers le reste du monde**
pass in on $if_in from $local_net proto tcp flags S/SA to any port domain keep state
pass in on $if_in from $local_net proto udp to any port domain keep state

Cette configuration semble être celle d'un routeur qui ne souhaite pas être joint lui-même mais qui autorise toutes les connexions initiées depuis le sous-réseau local. Ce principe marcherait tout à fait avec ipfilter mais la façon dont pf gère les états fait que ça ne marche pas. CF exercice 5 pour une explication et une solution.