TD sur les pare-feux

1 Pare-feu au niveau paquet

Exercice 1 : Donnez la configuration nftables pour bloquer tout le trafic à destination de la machine locale. Donnez ensuite la (ou les) commande(s) pour autoriser les connexions sur le port 80 (http).

Exercice 2 : Donnez la configuration nftables pour bloquer tout le trafic qui transite par la machine (routeur). Donnez ensuite la (ou les) commande(s) pour autoriser les connexions provenant de l'interface eth0 et à destination du port 80 (http) vers eth1.

Exercice 3 : Vous voulez protéger votre machine personnelle (sous Linux). Celle-ci possède une interface réseau eth0 sur laquelle ne sont connectées que vos machines auxquelles vous faites toute confiance. L'interface eth1 vous relie à l'Internet. Donnez la configuration nftables pour :

- vous protéger de l'IP-spoofing (pensez à créer une chaîne)
- créer une chaîne qui va bloquer des ports bien connus pour générer du trafic indésirable (par exemple 135-139 et 4662)
- accepter le retour des connexions que vous avez initié
- autoriser une connexion sur le port ssh de votre machine mais uniquement depuis une adresse IP fixée (1.30.30.30).
- enregistrer dans le journal les connexions ssh qui s'effectuent sur votre machine
- garder une trace dans le journal des tentatives de connexions qui échouent
- renvoyer un message d'erreur ICMP si éventuellement vous refusez un datagramme (mais uniquement sur eth0)

Exercice 4 : Vous devez cette fois protéger un réseau en configurant la machine linux qui sert de routeur. Celle-ci possède une interface réseau eth0 sur laquelle sont connectées vos machines fixes, une interface eth1 sur laquelles sont connectées vos ordinateurs portables et une interface eth2 reliée à l'internet. Donnez la configuration nftables pour :

- éviter les attaques de type IP spoofing
- autoriser un accès SSH sur le pare-feu depuis l'unique machine de l'administrateur
- laisser vos machines accéder aux serveurs DNS
- laisser votre relai de messagerie accéder au relai de votre FAI
- autoriser l'accès à votre serveur web depuis l'internet
- autoriser votre proxy web à dialoguer avec l'internet
- interdire toute connexion web qui ne passerait pas par le proxy
- autoriser les connexions SSH, POP3, SMTP, WWW depuis votre deuxième site
- envoyer un message ICMP d'erreur quand vous rejetez un datagramme et si ce n'est pas trop dangereux
- le réseau des portables ne peut pas échanger de datagramme avec le réseau des machines fixes (sauf pour échanger ou recevoir du courrier électronique)

Serveur DNS : 1.1.1.4
Relai de messagerie du FAI : smtp.fai.fr
Votre réseau : 10.1.0.0/17 pour les fixes, 10.1.128.0/17 pour les portables
Votre relai de messagerie : mail.mondomaine.fr
Votre proxy web : 10.1.0.10 et 10.1.128.10
Deuxième site : 10.2.0.0/16
Machine de l'administrateur : master.mondomaine.fr

Exercice 5 : Écrivez un mini-proxy HTTP qui se contente de transmettre les requêtes GET uniquement et bloque au passage tous les cookies (en-têtes Set-Cookie dans les réponses).