Etablissement : ENP d'Oran
Département : Génie des Systèmes
Module : Sécurité des systèmes d'information

Firewall

Le réseau de la **figure 1** montre l'interconnexion d'un réseau interne avec un réseau externe via un firewall (par feu) équipé de deux interfaces eth0 et eth1.

Le réseau interne est connecté à l'interface eth0 et le réseau externe est connecté à l'interface eth1. La machine I appartient au réseau interne et la machine E appartient au réseau externe

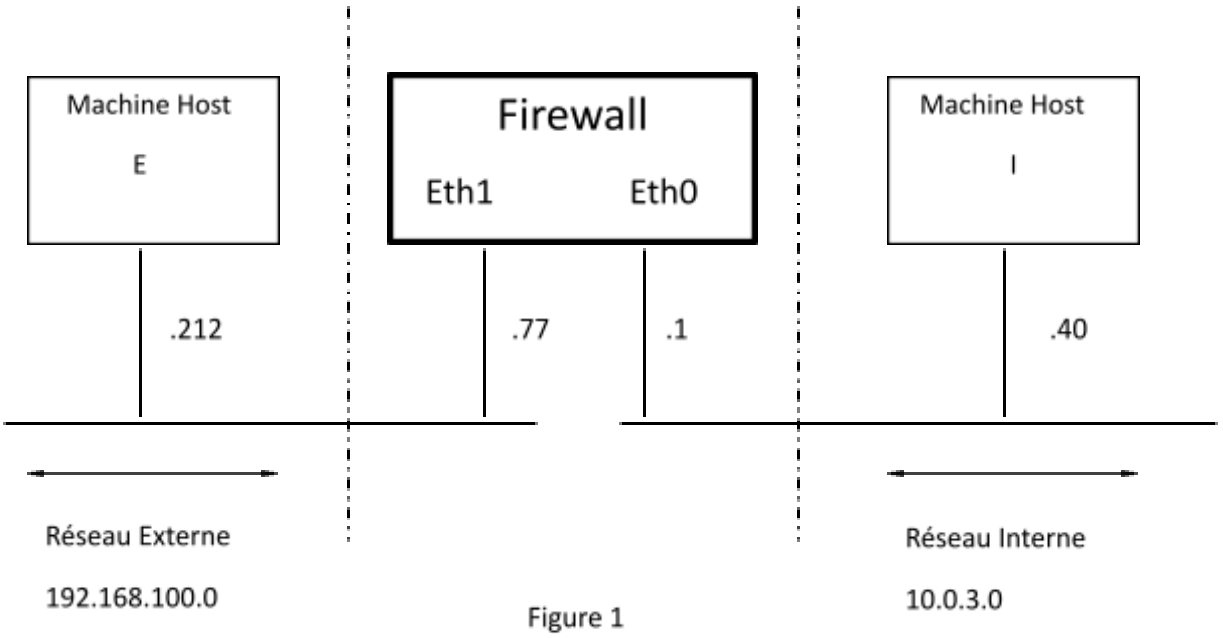

Figure 1

A. Si on exécuté depuis la machine l'@IP 10.0.3.40 la règle suivante :

Iptables −A INPUT −i lo −j DROP, avec lo : loopback (boucle locale) quel est son effet ?

- Si on exécute juste après cette règle : ping 127.0.0.1, quelle serait la réponse ?
  Requête accepté
- Si exécute juste après cette règle : ping www.yahoo.fr , quelle serait la réponse ?
  Requête refusé

B. Sécurité de la machine host I d'@IP 10 .0.3.40 :

L'objectif est de sécuriser le trafic entrant (INPUT) et le trafic sortant (OUTPUT) de cette machine a l'aide de iptables, établir les règles correspondantes à la politique de sécurité suivante :

Etablissement : ENP d'Oran
Département : Génie des Systèmes
Module : Sécurité des systèmes d'information

La politique par défaut est de n'autoriser aucun trafic entrant et sortant à la machine
I

Réponse :

Iptables –P INPUT DROP

Iptables –P OUTPUT DROP

Iptables –P FORWARD DROP

1. Laisser entrer et sortir tout paquet correspondant aux connexions établies ou en rapport avec d'autres connexions existantes

   Réponse :

Iptables –A INPUT –m state –state ESTABLISHED , RELATED -J ACCEPT

Iptables –A OUTPUT –m state –state ESTABLISHED , RELATED -J ACCEPT

2. Considérer juste les connexions entrantes suivantes :
   a. Connexion SSH (TCP : 22) depuis les machines du réseau interne

   Réponse :

Iptables –A INPUT –s 10.0.3.0/24 –p tcp –sport 22 –m state –state NEW -J ACCEPT

   b. Connexion TELNET (TCP : 23) depuis locales (Cad depuis l'interface loopback)

Iptables –A INPUT –I lo –p tcp –sport 23 –m state –state NEW -J ACCEPT

4 . Considérer juste les connexions entrantes suivantes :
   a. Connexion HTTP (TCP : 88) à un serveur web interne d'@IP 10.0.3.100

Iptables –A OUTPUT –d 10.0.3.100 –p tcp –dport 80 –m state –state NEW -J ACCEPT

   b. Connexion DNS (UDP : 53) à un serveur DNS interne d'@IP 10.0.3.200

Iptables –A OUTPUT –d 10.0.3.200 –p udp –dport 53 –m state - -state NEW -J ACCEPT

Etablissement : ENP d'Oran
Département : Génie des Systèmes
Module : Sécurité des systèmes d'information

C. Sécurité du réseau interne (firewall du réseau) : L'objectif est de sécuriser le réseau interne 10.0.3.0/24 à l'aide du firewall de la figure 1 ci-dessus

A l'aide de iptables, établir les règles correspondantes à la politique de sécurité suivante :

1. Politique par défaut : interdire tout trafic entrant, sortant et relayé par le firewall .

   Réponse :

   Iptables –P INPUT DROP

   Iptables –P OUTPUT DROP

   Iptables –P FORWARD DROP

2. Autorisation de (forwarding) de paquets suivants provenant ou à destination du réseau interne via l'interface eth0
   - Paquet correspondants aux connexions déjà établies
   - Paquets en rapport avec d'autres connexions existantes

Iptables –A FORWARD –o eth0 –d 10.0.3.0/24 –m state - -state ESTABLISHED , RELATED -J ACCEPT

Iptables –A FORWARD –i eth0 –s 10.0.3.0/24 –m state - -state ESTABLISHED , RELATED -J ACCEPT

3. Autorisation de connexions http (TCP /80) sortantes (c a d depuis le réseau interne vers le réseau externe)

Iptables –A FORWARD –i eth0 –s 10.0.3.0/24 -p tcp –dport 80 –m state - -state NEW - J ACCEPT