Correction TD Firewall

Exercice 1

Une entreprise dispose d'un pare-feu pour limiter l'accès depuis et vers les machines de son réseau interne. L'architecture du réseau de l'entreprise comprend également une zone démilitarisée (DMZ) pour le déploiement des serveurs Web et DNS propres à l'entreprise. La politique de sécurité appliquée par le pare-feu est décrite par le tableau 1.

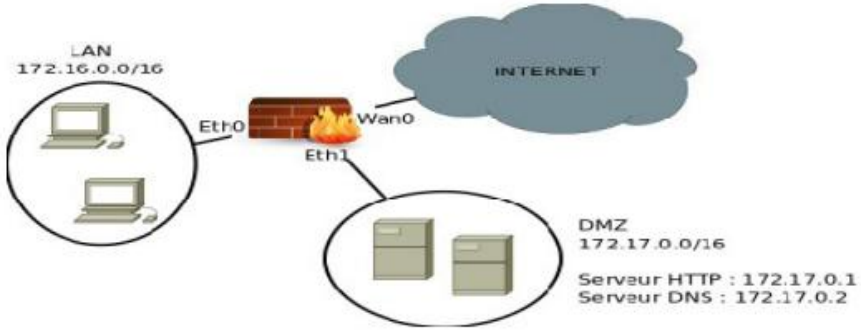

tableau 1

N°	Interface entrée	Interface sortie	Adr IP source	Adr IP destination	Protocole	Port source	Port dest	Action
1	Eth0	Eth1	172.16.0.0	172.17.0.1	TCP	> 1024	80	Accepter
2	Eth1	Eth0	172.17.0.1	172.16.0.0	TCP	80	> 1024	Accepter
3	Eth0	Eth1	172.16.0.0	172.17.0.2	UDP	> 1024	53	Accepter
4	Eth1	Eth0	172.17.0. 2	172.16.0.0	UDP	53	> 1024	Accepter
5	Wan0	Eth1	*	172.17.0.1	TCP	> 1024	80	Accepter
6	Eth1	Wan0	172.17.0.1	*	TCP	80	> 1024	Accepter
7	Eth0	Wan0	172.16.0.0	*	TCP	> 1024	80	Accepter
8	Wan0	Eth0	*	172.16.0.0	TCP	80	> 1024	Accepter
9	*	*	*	*	*	*	*	Refuser

1. Donner la politique correspondante à chaque paire de règles (1-2), (3-4), (5-6) et (7-8)

(1-2) : Autoriser les machines du LAN à se connecter au serveur web de la zone DMZ.

(3-4) : Autoriser les machines du LAN à se connecter au serveur DNS de la zone DMZ.

(5-6) : Autoriser les machines de l'extérieur (depuis internet) à se connecter au serveur web de la zone DMZ.

(7-8) : Autoriser les machines du LAN à se connecter aux serveurs web de l'internet.

2. Préciser la règle qui vérifiera chacun des paquets suivants et dites si le paquet sera accepté ou refusé

p1- IP sce : 172.16.0.30 IP Dest : 12.230.24.45 Prot : TCP Port sce :1045 Port dest : 443 →N9→trafic refusé

p2- IP sce : 172.16.10.5 IP Dest : 172.17.0.2 Prot : UDP Port sce :6810 Port dest : 53 →N3→accepté

p3- IP sce : 140.10.2.1 IP Dest : 172.17.0.1 Prot : TCP Port sce :8000 Port dest : 80 →N5→accepté

p4- IP sce : 17.14.3.3 IP Dest : 172.17.0.2 Prot : UDP Port sce :6000 Port dest : 53 →N9→refusé

p5- IP sce : 172.17.0.1 IP Dest : 1.2.3.4 Prot : TCP Port sce :80 Port dest : 9999 →N6→accepté

3. Ajouter les règles Iptables permettant d'établir la politique suivante :

a) La machine jouant le rôle de firewall doit pouvoir être joignable via SSH depuis le LAN.

 # iptables -A INPUT –i Eth0 -p tcp - -dport 22 -s 172.16.0.0/16 -j Accept

 # iptables -A OUTPUT –o Eth0 -p tcp - -sport 22 -m state - -state ESTABLISHED,RELATED -j Accept

b) Les machines du LAN doivent pouvoir pinger une machine sur Internet et les serveurs de La DMZ.

Les machines du LAN doivent pouvoir pinger les serveurs de La DMZ.

 # iptables -A Forward –i Eth0 –o Eth1 -p icmp - -icmp-type echo-request -j Accept

 # iptables -A Forward –i Eth1 –o Eth0 -p icmp --icmp-type echo-reply -j Accept

Les machines du LAN doivent pouvoir pinger une machine sur Internet

 # iptables -A Forward –i Eth0 –o Wan0 -p icmp - -icmp-type echo-request -j Accept

 # iptables -A Forward –i Wan0 –o Eth0 -p icmp - -icmp-type echo-reply -j Accept

c) Les machines du LAN doivent pouvoir télécharger des fichiers de l'internet via FTP.

 # iptables -A Forward –i Eth0 –o Wan0 -p Tcp --dport 21 -j Accept

 # iptables -A Forward –i Wan0 –o Eth0 -m state - -state ESTABLISHED,RELATED -j Accept