Iptables

I) Introduction :

Il existe trois tables :

Filter : C'est la table par défaut qui permet le filtrage des paquets. Elle ne modifie pas le contenu des paquets. Elle est constituée de trois chaînes : INPUT, OUTPUT et FORWARD.

Nat : Cette table effectue le masquerading. Elle est constituée de trois chaînes internes : PREROUTING, OUTPUT et POSTROUTING..

Mangle : Cette table permet de faire certaines modifications d'un paquet, par exemple de modifier sa priorité. Elle est constitué de deux chaînes . PREROUNTIG et OUTPUT.

II) Les chaînes prédéfinies :

Les noms des chaînes internes sont en majuscule.

Un paquet qui transite par le parefeu passe par la chaîne FORWARD.

Un paquet provenant du parefeu passe par la chaîne OUTPUT.

Un paquet à destination du parefeu passe par la chaîne INPUT.

La chaîne PREROUTING permet de modifier un paquet dès qu'il entre dans le système avant qu'il soit routé.

La chaîne POSTROUNTING permet de modifier un paquet juste avant sa sortie du système après qu'il soit passé dans le module de routage.

III) Les politiques :

ACCEPT : On laisse passer le paquet.

DROP : Le paquet est abandonné.

QUEUE : Le paquet est transféré dans l'espace utilisateur, si le noyau le permet.

RETURN : La politique finale de la règle s'applique sans exploiter les règles suivantes.

IV) Options utilisées avec les commandes :

- A : Ajouter une règle à une chaîne.

- I : Ajouter une règle en tête du filtre.

- D : Effacer une règle.

-N : Créer une chaîne utilisateur.

- P : Fixer la politique d'une chaîne.

V) Options utilisés avec les actions :

-p : Indiquer un protocole.

-s : Indiquer une adresse source.

-d : Indiquer une adresse destination.

- i : Spécifie l'interface réseau dans le cas des paquets entrants.

- o : Spécifie l'interface réseau dans le cas des paquets sortants.

[!]-f : La règle ne s'applique qu'aux fragments suivants.

-j : Préciser ce que l'on fait si la règle s'applique, soit une politique, soit une chaîne utilisateur.

VI) Les options étendues :

-- sport : Spécifier le port source.

--dport : Spécifier le port destination.

--icmp-type [!] : Spécifier un type de paquet ICMP.

--mac-source [!] : Spécifier une trame réseau.

--state : Liser les états qui doivent correspondre. Les états possibles sont :

INVALID : Le paquet n'est pas associé à une connexion connue.

ESTABLISHED : Le paquet est associé à une connexion connue.

NEW : Le paquet est associé à une nouvelle connexion.

RELATED : Le paquet appartient à une nouvelle connexion mais qui est associé à une connexion établie (ftp par exemple).

VII) Exemples :

Voir les règles : iptables –L

Sauver les règles : iptables-save > nom fichier

Restaurer sauvegarde : iptables-restore < nom fichier

Rejeter les paquets transitant par le parefeu et qui proviennent du réseau 173.17.0.0/16 et qui entrent par l'interface eth1 :

Iptables –A FORWARD –i eth1 –s 173.17.0.0/16 –j DROP

Ajouter une règle qui accepte les paquets transitant par le parefeu et qui sont destinés au serveur de messagerie (port tcp 25) qui possède comme IP 173.17.5.3 :

Iptables –A FORWARD -p tcp -d 173.17.5.3 --dport 25 –j ACCEPT

Ajouter une règle qui rejette les paquets de connexion TCP destines au réseau 173.17.0.0/16 qui transitent par le parefeu :

Iptables –A FORWARD -p tcp --syn –d 173.17.0.0/16 –j DROP

Héberger un dns/mail/http/ftp sur une machine dédié autre que le firewall :
iptables –t nat –I PREROUTING –d [ip firewall] –p tcp --dport 25 –j DNAT –to [ip privé serveur mail]

iptables –t nat –I POSTROUTING –s [ip privé serveur mail] –p tcp --sport 25 –j SNAT –to [ip firewall]

Héberger un dns/mail/http/ftp sur le firewall :
Mail : iptable –i INPUT –p tcp --dport 25 –j ACCEPT

DNS : iptable –i INPUT –p udp --dport 53 –j ACCEPT

Test :

eth0 c'est la carte relié sur le réseau interne. 10.176.164.1/24 pas de passerelle.
eth1 c'est la carte relié au retour. 192.168.1.11
Routeur : 192.168.1.1
Portable 10.176.164.2/24 pas de passerelle.

Avant chaque test, vérifier que les cartes réseaux sont bien paramétrées :
ifconfig eth0
ifconfig eth1

Si, elles ne sont pas montés :
sudo ifup eth0
sudo ifup eth1

Puis vérifier à nouveau à l'aide de ifconfig

Nettoyage iptables :
sudo iptables -F
sudo ptables -X

Par défaut on DROP tous les paquets :

sudo iptables -A INPUT -j DROP
sudo iptables -A OUTPUT -j DROP
sudo iptables -A FORWARD -j DROP

Le ping localhost ainsi que sur le routeur (192.168.1.1) et le portable (10.176.164.2) ne fonctionne pas

Vérifions les règles prises en compte à l'aide de iptables -L :

```
cyrille@Patrontueur:~$ sudo iptables -L

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       0    --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       0    --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       0    --  anywhere             anywhere

cyrille@Patrontueur:~$
```

Autoriser pour l'interface lo les connexions entrantes (1ere ligne) et sortantes (2 éme ligne) :

```
sudo iptables -I OUTPUT -o lo -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
sudo iptables -I INPUT -i lo -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
```

Le ping localhost fonctionne maintenant :

Autoriser pour l'interface eth1 (vers le routeur) les connexions entrantes (2 éme ligne) et sortantes (1 ére ligne) :

```
sudo iptables -I OUTPUT -o eth1 -s 192.168.1.0/24 -d 192.168.1.0/24 -j ACCEPT
sudo iptables -I INPUT  -i eth1 -s 192.168.1.0/24 -d 192.168.1.0/24 -j ACCEPT
```

Le ping sur le routeur (192.168.1.1) fonctionne maintenant :

Autoriser pour l'interface eth0 (réseau local) les connexions entrantes (2 éme ligne) et sortantes (1 ére ligne) :

```
sudo iptables -I OUTPUT -o eth0 -s 10.176.164.0/24 -d 10.176.164.0/24 -j ACCEPT
sudo iptables -I INPUT  -i eth0 -s 10.176.164.0/24 -d 10.176.164.0/24 -j ACCEPT
```

Test ping depuis le portable sur 10.176.164.1fonctionne.

Pour le moment un ping sur internet ne fonctionne toujours pas :

Autoriser pour l'interface eth1 (interface relié au routeur) de surfer sur internet port 80 :

```
sudo iptables -I OUTPUT -o eth1 -s 192.168.1.0/24 -p tcp --dport 80  -j ACCEPT
sudo iptables -I INPUT  -i eth1 -d 192.168.1.0/24 -p tcp --sport 80  -j ACCEPT
```

Lancer un navigateur internet ou faire un lynx http:\\www.google.fr.

Autoriser pour l'interface eth1 (interface relié au routeur) de surfer sur internet port 443 (https) :

```
sudo iptables -I OUTPUT -o eth1 -s 192.168.1.0/24 -p tcp --dport 443 -j ACCEPT
sudo iptables -I INPUT -i eth1 -d 192.168.1.0/24 -p tcp --sport 443 -j ACCEPT
```

Pour vérifier si ça marche, connectez vous sur un site sécurisé (banque, impôts...).

Autoriser pour eth1 le relevé du courrier électronique (POP port 110) :

```
sudo iptables -I OUTPUT -o eth1 -s 192.168.1.0/24 -p tcp --dport 110  -j ACCEPT
sudo iptables -I INPUT  -i eth1 -d 192.168.1.0/24 -p tcp --sport 110  -j ACCEPT
```

Pour le test, lancer votre logiciel de messagerie et de relever le courrier.

Autoriser pour eth1 l'envoi du courrier électronique (SMTP port 25) :

```
sudo iptables -I OUTPUT -o eth1 -s 192.168.1.0/24 -p tcp --dport 25  -j ACCEPT
sudo iptables -I INPUT  -i eth1 -d 192.168.1.0/24 -p tcp --sport 25  -j ACCEPT
```

Autoriser pour Eth1 l'accès à un serveur teamspeak (pour notre cas c'est le port 8761) :

```
sudo iptables -I OUTPUT -o eth1 -s 192.168.1.0/24 -p udp --dport 8761  -j ACCEPT
sudo iptables -I INPUT  -i eth1 -d 192.168.1.0/24 -p udp --sport 8761  -j ACCEPT
```

Ne pas autoriser le ping :

interdire tout paquet entrant correspondant à un ping :
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

interdire toute réponse à un ping :
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP