R3.06 – Architecture des réseaux

HOWTO – iptables

1 – Syntaxe générale

La commande **iptables** permet d'agir sur la configuration du pare-feu du même nom. La commande en elle-même ne va pas accepter, logguer ou rejeter des messages réseaux : elle va agir sur les règles du pare-feu qui lui s'occupera de traiter les messages réseaux en fonction de sa configuration.

iptables *commande chaîne* [*critères*] [-j *action*]

A. Commandes

-A (Append) : ajoute une règle à la fin de la chaîne mentionnée.
-D *numéro* (Delete) : efface la règle désignée par *numéro*.
-F (Flush) : vide la chaîne.
-I *numéro* (Insert) : ajoute une règles à la position correspondant à numéro.
-L (List) : liste le contenu des chaînes.
-P (Policy) : définit le comportement par défaut (à DROP ou ACCEPT, jamais LOG).
-R *numéro* (Replace) : remplace la règle désignée par *numéro*.

B. Chaînes

INPUT : Tout message à destination de la machine exécutant le pare-feu
OUTPUT : Tout message provenant de la machine exécutant le pare-feu
FORWARD : Tout message passant par (routage) la machine exécutant le pare-feu

C. Critères

-d *@ip* : désigne une adresse IP de destination. Il est possible de désigner soit l'adresse précise d'une machine, soit un ensemble d'adresses correspondant à un sous-réseau.

-s *@ip* : désigne une adresse IP source. Il est possible de désigner soit l'adresse précise d'une machine, soit un ensemble d'adresses correspondant à un sous-réseau.
-i interface : désigne une interface d'entrée sur la machine exécutant le pare-feu (eth0, eth1, etc.)
-o interface : désigne une interface de sortie sur la machine exécutant le pare-feu
-p protocole : désigne un protocole correspondant à la couche TCP/UDP (Transport), c'est à dire généralement ICMP, DHCP, ARP, TCP et/ou UDP.
Si les protocoles UDP ou TCP sont désignés, il est possible de préciser les numéros de port en source ou destination :

--dport numéro : numéro de port de destination
--sport numéro : numéro de port source

D. Actions

ACCEPT : Le message est accepté, il sera donc transmis ou traité normalement.
DROP : Le message est rejeté. Il sera donc détruit.
LOG : Le message est loggué (enregistré dans un fichier de journalisation) et le pare-feu continuera à traiter les règles suivantes de la chaîne.

2 – Exemples d'utilisation

iptables -L FORWARD : affiche le contenu complet de la chaîne FORWARD
iptables -F INPUT : supprime toutes les règles de la chaîne INPUT (mais ne réinitialise pas son comportement par défaut).
iptables -P OUTPUT ACCEPT : définit le comportement par défaut de la chaîne OUTPUT à ACCEPT
iptables -A FORWARD -p icmp -j DROP : ajoute en fin de chaîne FORWARD une règle indiquant que tout message du protocole icmp doit être rejeté.
iptables -I 5 INPUT -d 192.168.1.5 -j LOG : ajoute en 5^{e} position de la chaîne INPUT une règle indiquant que si l'adresse de destination du message est 192.165.1.5 alors il doit être journalisé.