Netfilter et Iptables

Le pare-feu dans un environnement Linux est composé de plusieurs modules implémentés en son noyau et l’ensemble est nommé Netfilter. Son rôle est de filtrer et /ou transformer les paquets qui circulent dans le trafic entrant et sortant de la machine. Il utilise différents outils de configuration intégrés selon le protocole employé. Étant donné le rôle central que joue le protocole IPv4 dans les communications réseaux, l’outil IPtables est souvent qualifié comme étant lui-même le pare-feu Linux. Dans les faits, c’est une interface « ligne de commandes » qui permet à l’utilisateur de configurer Netfilter et sert de commande à tout faire.

Tous les paquets testés passent à travers des tables. Chacune d’entre elles agit comme une file d’attente et est dédiée à un type de traitement des paquets. Aux tables sont associé ou non cinq chaînes de base prédéfinies : PREROUTING, INPUT, FORWARD, OUTPUT et POSTROUTING. Chaque chaîne contiendra à son tour une cible (target) qui spécifie une action à effectuer sur le paquet comme par exemple ACCEPT, DROP, REJECT, LOG, DNAT, SNAT ou MASQUERADE. Ensuite elle peut contenir ou non des règles définies par des options de correspondances ou d’opérations constituant ainsi un filtre spécifique. L’ordre des règles est important puisque chaque paquet traverse systématiquement les chaînes examinant si une règle lui correspond ou non. Si c’est le cas la règle sera appliquée et le traitement arrêtera. Sinon le paquet passera à la suivante. Si aucune règle n’a arrêté le paquet la cible par défaut de la chaîne sera appliquée. L’administrateur peut créer autant de chaînes et de règles qu’il le désire. IPtables permet de consulter ou modifier les tables, les chaînes et les règles selon nos besoins.

Netfilter est constitué de 4 tables qui lui permettent de remplir ses fonctions.

1-La première table (MANGLE) par laquelle passe le paquet permet de lui apporter des modifications, leur appliquant ainsi un traitement spécial. Ceci peut influencer d’autres règles contenues dans les tables NAT et de filtrage. Elle contient les cinq chaînes prédéfinies.

2-La deuxième table est celle qui gère la translation d’adresse réseau (NAT). Elle permet de configurer la gestion de l’adressage lorsqu’on désire utiliser des adresses privées au sein du réseau interne. Or pour router les paquets de données sur un réseau externe, ceux-ci doivent être dotés d’une adresse publique. Le nating permet donc d’associer une adresse publique à une adresse privé. Elle contient les chaînes suivantes :

-chaîne PREROUTING (pré-routage) : principalement utilisé pour le DNAT (destination NAT ) dans lequel on change l'adresse de destination des paquets provenant du réseau public en une adresse privée du réseau local.

-chaîne POSTROUTING (post-routage) : utilisé pour le SNAT (source NAT) et qui consiste à changer une adresse privée source d’un paquet sortant avec une adresse source publique.

-chaîne OUTPUT : utilisé pour traduire les adresses des paquets générés par le pare-feu.

3- La table de filtrage (FILTER) sert principalement de fonctions de pare-feu. Elle spécifie les règles de trafic en indiquant par quels ports de la machine le paquet peut transiter. Elle est la table par défaut si la chaine n’est associée à aucune table. Elle a trois chaînes prédéfinies :

-chaîne FORWARD : filtre et transfère les paquets destinés à une machine derrière le pare-feu. Donc qui le traversent.

-chaîne INPUT : filtre les paquets destinés au pare-feu.

- chaîne OUTPUT : filtre les paquets qui ont pour origine le pare-feu.

4- La table (RAW) est principalement utilisée pour marquer les paquets qui doivent ou non être vérifiés par le système de traçage de connexion. Celui-ci permet de connaître l’état d’une connexion spécifique et ainsi de contrôler plus facilement qui ou quoi est autorisé à démarrer de nouvelles sessions.

L’outil de configuration de pare-feu IPtables est sans doute le plus célèbre de l’environnement Linux. Il est largement supporté par la communauté qui vante sa souplesse et sa simplicité de configuration. Les différentes combinaisons qu’il permet de réaliser font de lui un des outils les plus puissants du marché.

Sources :

[http://profdinfo.com/web/420-128-LG/Section%204.html#43](http://profdinfo.com/web/420-128-LG/Section%204.html" \l "43)

<http://www.inetdoc.net/guides/iptables-tutorial/statemachine.html>

Guide de configuration Netfilter-iptables - Version du 10 Juin 2009- PDF - REFERENCE: OPPIDA/DOC/2009/AUA/534/1.4

Netfilter. (2012, mai 6). *Wikipédia, l'encyclopédie libre*. Page consultée le 20:05, juin 23, 2012 à partir de <http://fr.wikipedia.org/w/index.php?title=Netfilter&oldid=78394038>.

<http://irp.nain-t.net/doku.php/130netfilter:010_architecture>

Iptables. (2011, septembre 29). *Wikipédia, l'encyclopédie libre*. Page consultée le 20:07, juin 23, 2012 à partir de <http://fr.wikipedia.org/w/index.php?title=Iptables&oldid=70549296>.

<http://www.commentcamarche.net/faq/1317-linux-installation-d-un-firewall#avant-propos>

Démonstration :

<http://www.howtoforge.com/nat_iptables>