iptables : pare-feu, routage et filtrage de paquets

- Objet : Fonctionement général d'iptables et exemples d'utilisation
- Niveau requis :
  avisé
- Commentaires : *iptables est une interface permettant de configurer le filtrage des paquets par le noyau Linux, il permet donc d'établir des firewall, de la redirection de ports, etc.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !
- Suivi :
  à-compléter
  - Création par captnfab 04/08/2013
  - Compléments par paskal 22/10/2015
- Commentaires sur le forum : ici[1)]

ip6table

Laurent1 : *Les commandes ip6tables pour sécuriser un serveur en ligne sont-elles les mêmes que les commandes iptables ou bien existerait-il quelque subtilité ?*

root@rkn : presque les mêmes, juste un 6 en plus :

ip6table.php

```
#! /bin/sh

ip6tables -t filter -P INPUT DROP
ip6tables -t filter -P OUTPUT DROP
ip6tables -t filter -P FORWARD DROP

ip6tables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

ip6tables -t filter -A INPUT -i lo -j ACCEPT
ip6tables -t filter -A OUTPUT -o lo -j ACCEPT


ip6tables -t filter -A INPUT -p icmpv6 --icmpv6-type echo-request -j
ACCEPT



ip6tables -t filter -A OUTPUT -p icmpv6 --icmpv6-type echo-request -j
ACCEPT
ip6tables -t filter -A OUTPUT -p icmpv6 --icmpv6-type echo-reply -j
ACCEPT
```

raleur : Dans les grandes lignes oui, mais il y a quelques subtilités.

1. Le protocole ICMP est remplacé par ICPMv6. Les noms des types et codes communs sont identiques (destination-unreachable, time-exceeded…) mais les numéros sont différents donc mieux vaut utiliser les noms. Le code fragmentation-needed du type destination-unreachable devient un type séparé packet-too-big.
2. Les requêtes et réponses ARP sont remplacées par un sous-ensemble de types ICMPv6 qui sont donc filtrés par ip6tables (alors que iptables ne filtre pas les paquets ARP, protocole distinct d'IPv4) :
    1. neighbor-solicitation
    2. neighbor-advertisement
    3. router-solicitation
    4. router-advertisement
3. La gestion de la fragmentation est différente en ICMPv6 car un routeur ne doit pas fragmenter un paquet ICMPv6 trop gros mais renvoyer systématiquement un message ICMPv6 packet-too-big. Mais la gestion des fragments et du réassemblage dans netfilter a changé au fil des versions du noyau. Attention donc, dans certaines chaînes ip6tables peut voir les fragments et dans d'autres le paquet reassemble, ce qui peut avoir un impact sur les règles de filtrage (seul le premier fragment contient les ports source et destination).

Bloquer ces messages peut empêcher toute connectivité IPv6. Ils ne sont pas gérés par le suivi d'état de connexion (conntrack) et ont l'état UNTRACKED.

Sources sur le forum : https://debian-facile.org/viewtopic.php?id=23658

Merci à **Laurent1**, **root@rkn** *et* **raleur** *pour ces informations actualisées.*

Introduction

Iptables est une interface en ligne de commande permettant de configurer Netfilter, le framework implémentant le pare-feu au sein du noyau Linux.
Il offre davantage de possibilités que ufw.

Pour une bonne compréhension d'iptables, il est conseillé de connaître auparavant le principe de fonctionnement des protocoles TCP et UDP.

Installation

Ordinairement, iptables est installé d'origine. Dans le cas contraire :

```
apt-get install iptables
```

Exemples d'utilisation

- iptables: un pare-feu pour un client
- iptables: un pare-feu pour une passerelle

Références

- Firewall et sécurité d'un réseau personnel sous Linux
- L'internet rapide et permanent
- IPtables et NetFilter, solution de pare-feu
- Les commandes iptables
- Netfilter/Iptables introduction
- Iptables

Liens utiles

En anglais :

- DebianFirewall, sur le wiki Debian.org
- iptables, sur le wiki Debian.org
- How To Iptables, sur netfilter.org
- Documentation Multilingue de Netfilter et Iptables, sur netfilter.org

En français :

- Pare-feu et partage de connexion Internet, sur formation-debian.via.ecp.fr
- Utiliser Iptables, sur netfilter.org
- Linux : IpTables !, sur “Mémoire Grise Libérée”
- Iptables Tutorial, sur inetdoc.net
- Supprimer une règle précise dans IPtables, sur IT-Connect

[1)]

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !