Jean Saquet – Université de Caen

Master d'Informatique

Réseaux avancés

Packet Filter (pf)

Bureau S3-354
Mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M2/rezo

Pf (Packet Filter)

C'est l'équivalent, pour OpenBSD, de Netfilter pour Linux. Comme lui et comme son nom l'indique, il s'agit d'un système de filtrage des paquets, autrement dit un pare-feu.
Il peut également effectuer des opérations de translation d'adresses, de redirection de trafic, ainsi que des possibilités de gestion de bande passante.
Il est activé par défaut, mais avec une règle qui laisse tout passer.

Pf - Contrôle

Le fichier de règles par défaut est /etc/pf.conf.
La commande pfctl permet de contrôler pf. (cf man pfctl)
par exemple :
Pfctl -e ou -d (Enable – Disable)
Pfctl -f <fichier> (Lecture d'un fichier de règles)
Pfctl -sr ou -ss ou -si ou -sa (Affichage des règles, des tables d'état, des stats, ou de tout)

Pf – Filtrage - Principe

On bloque ou on laisse passer (block ou pass).
La nuance comme avec drop et reject de Iptables se règle en précisant block drop ou block return.
Les règles sont bien entendu ordonnées, mais par défaut TOUTES les règles sont évaluées et la DERNIERE qui correspond s'applique.
Toutefois l'option quick permet de stopper l'évaluation sur une règle particulière.

Pf – Filtrage - Paramètres

action [*direction*] [log] [quick] [on *interface*] [*af*] [proto *protocol*]
[from *src_addr* [port *src_port*]] [to *dst_addr* [port *dst_port*]]
[flags *tcp_flags*] [*state*]

- direction : in ou out
- interface(s) concernée(s)
- af : inet ou inet6
- proto : tcp, udp, icmp, icmp6, numéro, ou mnémonique de /etc/protocols, liste
- adr et ports source, dest, flags tcp
- state : cf. plus loin

Pf – Etat

Pf peut conserver l'état des connexions, dans une table.
On teste ainsi si un packet correspond à une connexion déjà autorisée. Donc pas de règle pour le retour.
Par défaut, toute règle pass crée une entrée dans la table d'états.
State a plusieurs options : keep (par défaut), no, modulate (gestion des nos séquences TCP initiaux), synproxy (proxy TCP)

Pf – Etat - précisions

Pour udp : time-out, configurable

Options de suivi pour le nombre maximum d'entrées dans la table créés par une règle, suivi des adresses Ips, …Ex :

```
pass in on $ext_if proto tcp to $web_server
    port www keep state
    (max 200, source-track rule, max-src-
nodes 100, max-src-states 3)
```

(total 200 états, 100 clients, 3 connexions par client)

Pf – filtrages fins

Mandataire TCP : permet d'éviter l'inondation de paquets SYN – à utiliser avec modération.
Blocage de paquets avec adresse usurpée :
- adresse arrivant manifestement via une mauvaise interface
- route de retour vers cette adresse ne correspondant pas à l'arrivée

Reconnaissance d'empreintes connexions TCP
Filtrage des options IP

Pf – Translation d'adresses

Option nat-to dans une règle pass, ou bien :
Règle match + règle pass :
- match définit le nat à appliquer pour des paquets vérifiant certaines conditions
- si une règle pass est rencontrée avec les mêmes conditions, on applique le nat au paquet
Permet de faire des exceptions à la règle nat

Nat permanent : binat-to, ports non modifiés
Ou bien redirection (rdr-to)

Pf – Divers

Pour simplifier l'écriture des règles, on peut utiliser des variables, des macros, des listes d'adresses, de ports, …

La syntaxe est assez souple et peut dans bien des cas être simplifiée.

Pour plus de détails, voir www.openbsd.org/faq/pf/fr

Pfsense

C'est une distribution de OpenBSD configurée principalement comme routeur et pare-feu, ce dernier étant évidemment basé sur PF.

Nous l'utiliserons sur les boitiers Alix, cette distribution étant proposée par le distributeur de ces machines.

Voir notamment le site www.pfsense.org.