BPF

Table of Contents

BPF (**B**erkeley **P**ackage **F**ilter), apparu pour la première fois en 1993 puis intégré au kernel en 1997 avec la version 2.1.75 est une petite machine virtuelle à l'intérieur du kernel où on peut y injecter des instructions pour faire des règles de filtrage réseau.

Avec **eBPF** arrive une extension des capacités de la VM et surtout une vraie interface avec celle-ci pour pouvoir y injecter du code C à exécuter.

XDP (e**X**press **D**ata **P**ath) est un chemin de données haute performance basé sur **eBPF** fusionné dans le noyau Linux depuis la version 4.8.[1]

L'idée derrière **XDP** est d'ajouter un premier hook dans le chemin RX du noyau, et de laisser un programme **eBPF** fourni par l'utilisateur décider du sort du paquet. Le hook est placé dans le pilote NIC juste après le traitement d'interruption et avant toute allocation de mémoire requise par la pile réseau elle-même, car l'allocation de mémoire peut être une opération coûteuse. Grâce à cette conception, **XDP** peut supprimer 26 millions de paquets par seconde par cœur avec du matériel de base

CONFIG_BPF_SYSCALL

Active l'appel système bpf() qui permet de manipuler les programmes et les cartes **eBPF** via des descripteurs de fichiers.

CONFIG_CGROUP_BPF

Autorise la liaison de programmes **eBPF** à un groupe de contrôle à l'aide de la commande bpf(2) syscall BPF_PROG_ATTACH.

Dans quel contexte ces programmes sont accessibles dépend du type de pièce jointe. Par exemple, les programmes attachés à l'aide de BPF_CGROUP_INET_INGRESS seront exécutés sur le chemin d'entrée des sockets inet.

CONFIG_BPF_JIT_ALWAYS_ON

Active le compilateur à la volée du kernel (JIT compiler) et supprime l'interpréteur **BPF** pour éviter l'exécution spéculative des instructions **BPF** par l'interpréteur

CONFIG_BPF_STREAM_PARSER

Autorisez la liaison de programmes **eBPF** à un groupe de contrôle à l'aide de la commande bpf (2) syscall BPF_PROG_ATTACH.

L'activation de cette option permet d'utiliser un analyseur de flux avec BPF_MAP_TYPE_SOCKMAP.

BPF_MAP_TYPE_SOCKMAP fournit un type de carte à utiliser avec les sockets réseau. Il peut être utilisé pour appliquer la politique de socket, implémenter des redirections de socket, etc..

CONFIG_XDP_SOCKETS

Les sockets **XDP** permettent un canal entre les programmes **XDP** et les applications de l'espace utilisateur.

CONFIG_XDP_SOCKETS_DIAG

Prise en charge de l'interface de surveillance des sockets **PF_XDP** utilisée par l'outil ss. En cas de doute, répondre Y.

CONFIG_BPF_KPROBE_OVERRIDE

Permet à **BPF** de remplacer l'exécution d'une fonction testée et de définir une valeur de retour différente. Ceci est utilisé pour l'injection d'erreur.