Filtrage et DNS : RPZ et XDP

Romain Cherré

11 octobre 2022

Contexte

- Résolutions de noms dans un réseau
- Serveurs ou machines clients utilisant des services externes
- Filtrage sur/avec protocole DNS

Plan

Section 1

Response Policy Zone (RPZ)

Filtrage du serveur DNS

Principe

Une zone décrivant le filtrage effectué sur les *requêtes* et *réponses* DNS
IETF Draft : draft-ietf-dnsop-dns-rpz-00

Les possibilités

Règles

- par l'adresse IP du client
  - 10.0.168.192.rpz-client-ip CNAME rpz-passthru.
  - 24.0.0.168.192.rpz-client-ip CNAME rpz-passthru.
- par le nom demandé (example.com CNAME rzp-passthru.)
- par l'adresse IP présente dans la réponse (1.0.168.192.rpz-ip CNAME .)
- par le nom ou l'IP du serveur autoritaire de la réponse initiale (ns.example.com.rpz-nsdname CNAME .)

Les possibilités

Actions

- NXDOMAIN (example.com CNAME .)
- NODATA (example.com CNAME *.)
- drop (example.com CNAME rpz-drop.)
- bascule sur TCP (example.com CNAME rpz-tcp-only.)
- remplace les données de la réponse
  - ad1.example.com CNAME garden.example.net.
  - bad2.example.com A garden-web.example.net.
  - bad2.example.com MX garden-mail.example.net.
- arrête l'application de la politique et laisse passer la requête/réponse
  - *.example.com CNAME rpz-passthru.
  - 32.1.2.0.192.rpz-client-ip CNAME rpz-passthru.

En pratique

Cas d'usage

- Réponses d'un serveur DNS externe : IPs RFC1918, IP réputation malveillante (blacklists), serveurs autoritaires malveillant (ex : Conficker)
- Requêtes : whitelist, blacklist
- Politique selon clients (ex : tags de Unbound)

Implémentaions

Bind, Unbound, PowerDNS,...

Section 2

Filtrage eBPF - XDP

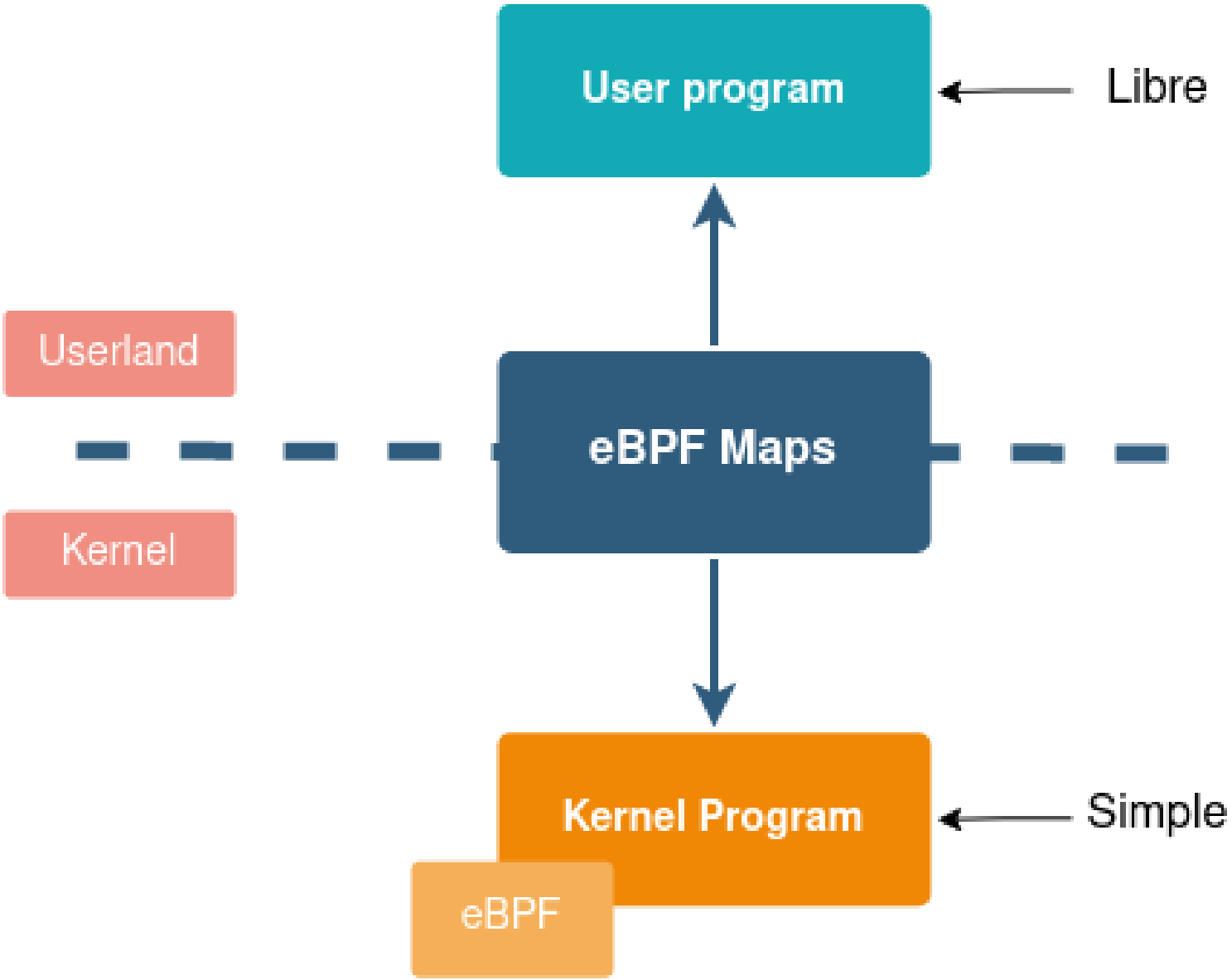
eBPF et XDP

eBPF

"eBPF is a [...] technology [...] that can run sandboxed programs in an operating system kernel"

- Limitations dues au vérifieur
- Interfaces avec le noyau : lire des variables à partir du contexte d'exécution d'une fonction
- Structures : array, hash map, ..., accessibles depuis l'espace utilisateur

eBPF


User program
Libre
Userland
eBPF Maps
Kernel
Kernel Program
Simple
eBPF

eXpress Data Path (XDP)

XDP

- Sous la forme d'un programme eBPF
- Filtre les paquets dès leur arrivée
- Possibilité d'offload sur le matériel
- Modifier les paquets
- Retourne une action

Liste des actions

- XDP_PASS : let the packet continue through the network stack
- XDP_DROP : silently drop the packet
- XDP_ABORTED : drop the packet with trace point exception
- XDP_TX : bounce the packet back to the same NIC it arrived on
- XDP_REDIRECT : redirect the packet to another NIC or user space socket via the AF_XDP address family

Filtrage

- Filtrage statique (whitelist, blacklist) sur les requêtes et réponses DNS
- Filtrage IP destination dynamique : le flux vers une IP destination est autorisé si l'IP a été résolue précédemment
- Combinaison des deux précédents : filtrage via des noms de domaines sans avoir à gérer les mises à jour (résolution fréquentes pour mettre à jour les IPSets ou sets)

En pratique

Cas d'usage

- adapté pour les serveurs dans des environnements hybrides ou utilisants des APIs externes au SI
- poste de travail : peut ne pas fonctionner dans certains cas : requêtes directement vers l'IP sans utilisation de nom de domaine (ex : application P2P, speedtest, etc)

Produits

- Calico, Cilium, *vos scripts*,. . .
- Scripts PowerDNS :
  - https ://github.com/PowerDNS/pdns/blob/master/contrib/xdp.py
  - https ://github.com/PowerDNS/pdns/blob/master/contrib/xdp-filter.ebpf.src

FIN

Questions ?