BPF and firewall: bpfilter to speed up iptables

Quentin Deslandes
Software Engineer

Meta

Agenda

1. About packet filtering: iptables
2. bpfilter: the kernel module
3. bpfilter: the userspace daemon
4. More in deep
5. Future work

Jérôme Petazzoni
@jpetazzo

OH: "In any team you need a tank, a healer, a damage dealer, someone with crowd control abilities, and another who knows iptables"

- Netfilter is the standard Linux firewall framework
- Slower than than BPF
- Easy to use

Jérôme Petazzoni
@jpetazzo

As it turns out, I should retire that tweet, since now we also need someone who knows eBPF, XDP, nftables ...

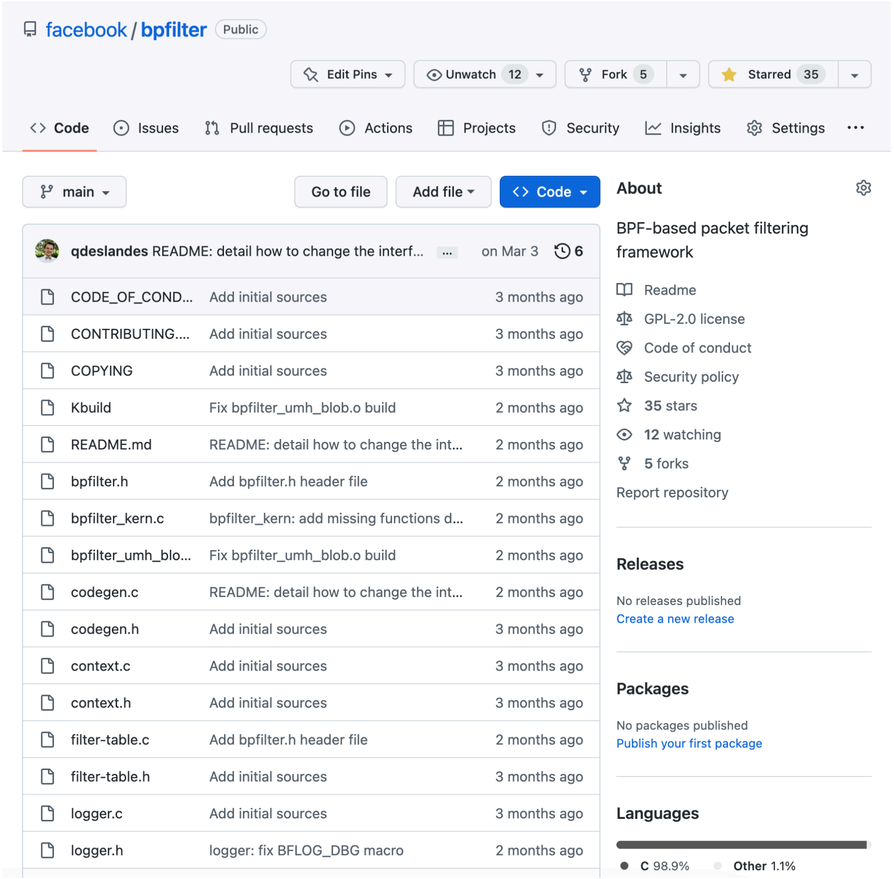
- “[PATCH v3 net-next 0/2] bpfilter”, by Alexei, David Miller, and Daniel Borkmann ([0])
  - Focusing on usermode helper
- “[PATCH bpf-next v2 00/13] bpfilter", by Dmitrii Banshchikov
  - Catch iptable’s getsockopt() calls
  - Generate BPF program

[0]: https://lore.kernel.org/lkml/20180522022230.2492505-1-ast@kernel.org/

[1]: https://lore.kernel.org/bpf/20210829183608.2297877-1-me@ubique.spb.ru/

Moving away from the usermode helper

- Transform bpfilter into a userspace daemon
  - Translating rules into a BPF program
  - Support packets/bytes counters
- PoC for iptables working with bpfilter



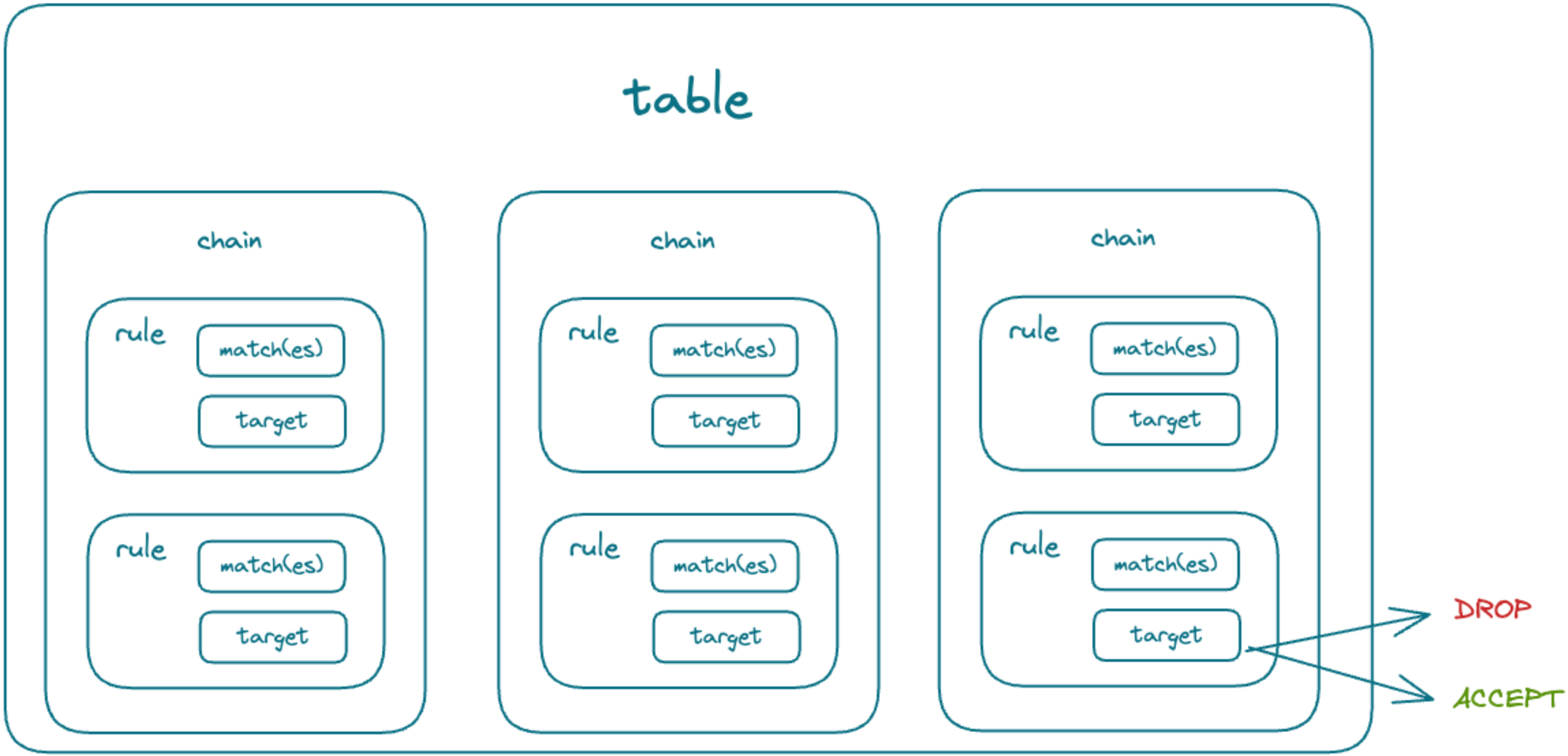
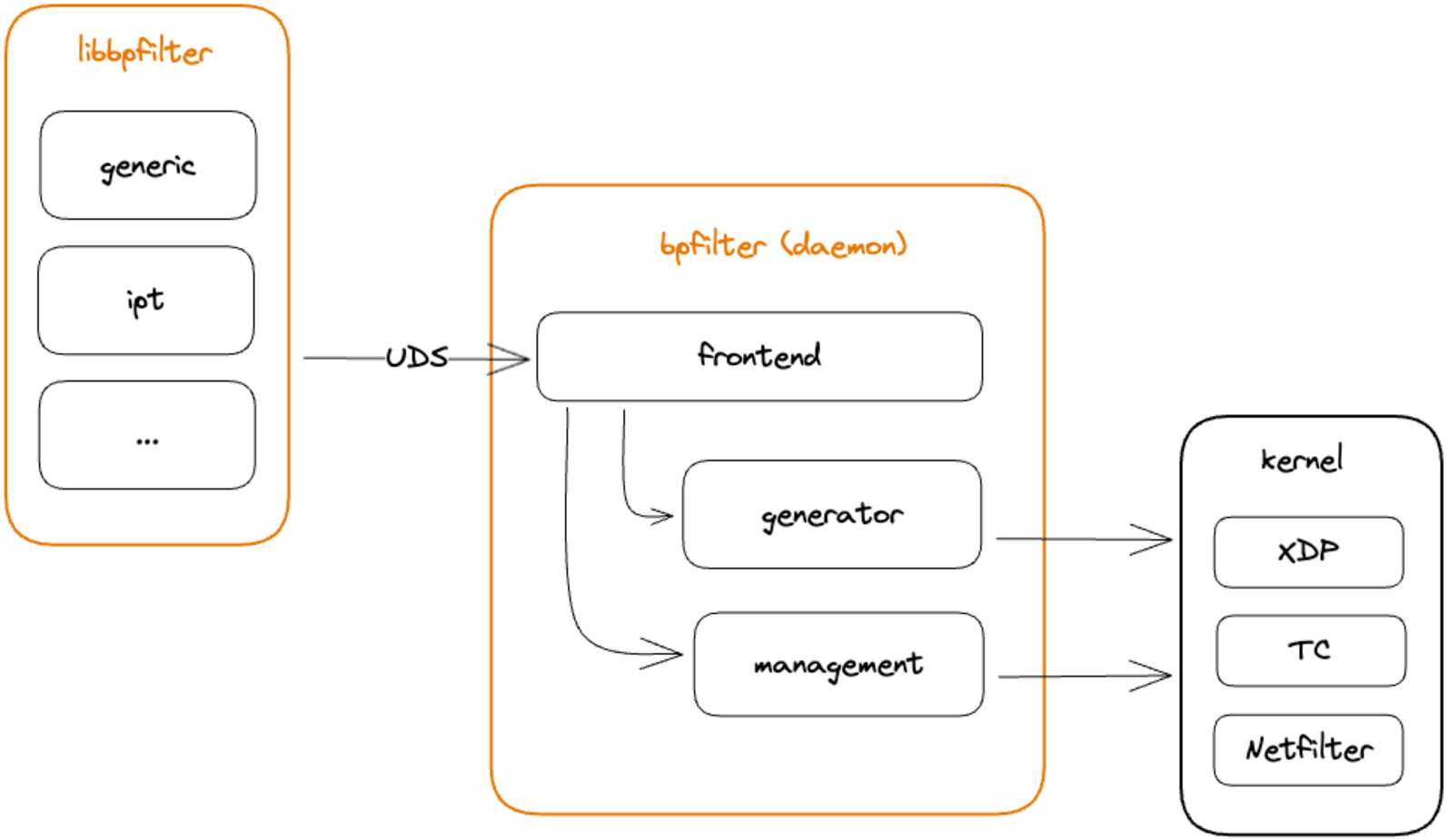


table
chain
rule
match(es)
target
rule
match(es)
target
chain
rule
match(es)
target
rule
match(es)
target
chain
rule
match(es)
target
rule
match(es)
target
DROP
ACCEPT


libbpfilter
generic
ipt
...
UDS
bpfilter (daemon)
frontend
generator
management
kernel
XDP
TC
Netfilter

What is coming?

- Support for Florian Westphal’s BPF_NETFILTER hooks
  - Add support for a new BPF flavour
  - Access the packet’s data through dyn_ptr
- Support for nftables data format
- User defined chains
- Extending iptables/nftables support


Meta