

BPF and firewall: bpfILTER to speed up iptables

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

facebook / bpfiler Public

Edit Pins Unwatch 12 Fork 5 Starred 35

Code Issues Pull requests Actions Projects Security Insights Settings

main Go to file Add file Code About

qdeslandes README: detail how to change the interf... on Mar 3 6

CODE_OF_COND...	Add initial sources	3 months ago
CONTRIBUTING...	Add initial sources	3 months ago
COPYING	Add initial sources	3 months ago
Kbuild	Fix bpfiler_umh_blob.o build	2 months ago
README.md	README: detail how to change the int...	2 months ago
bpfiler.h	Add bpfiler.h header file	2 months ago
bpfiler_kern.c	bpfiler_kern: add missing functions d...	2 months ago
bpfiler_umh_blo...	Fix bpfiler_umh_blob.o build	2 months ago
codegen.c	README: detail how to change the int...	2 months ago
codegen.h	Add initial sources	3 months ago
context.c	Add initial sources	3 months ago
context.h	Add initial sources	3 months ago
filter-table.c	Add bpfiler.h header file	2 months ago
filter-table.h	Add initial sources	3 months ago
logger.c	Add initial sources	3 months ago
logger.h	logger: fix BFLOG_DBG macro	2 months ago

About

BPF-based packet filtering framework

- Readme
- GPL-2.0 license
- Code of conduct
- Security policy

35 stars
12 watching
5 forks

Report repository

Releases

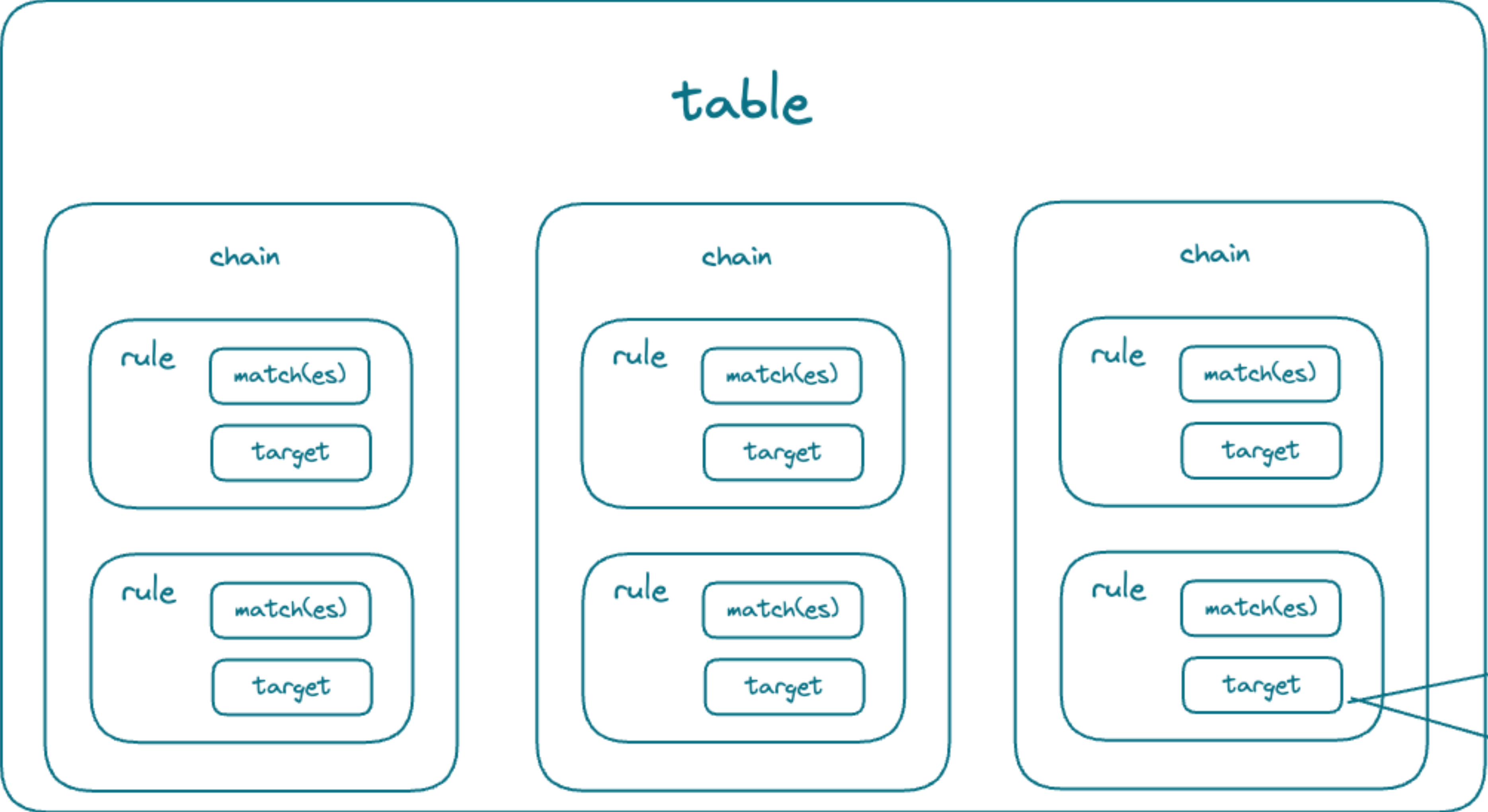
No releases published
[Create a new release](#)

Packages

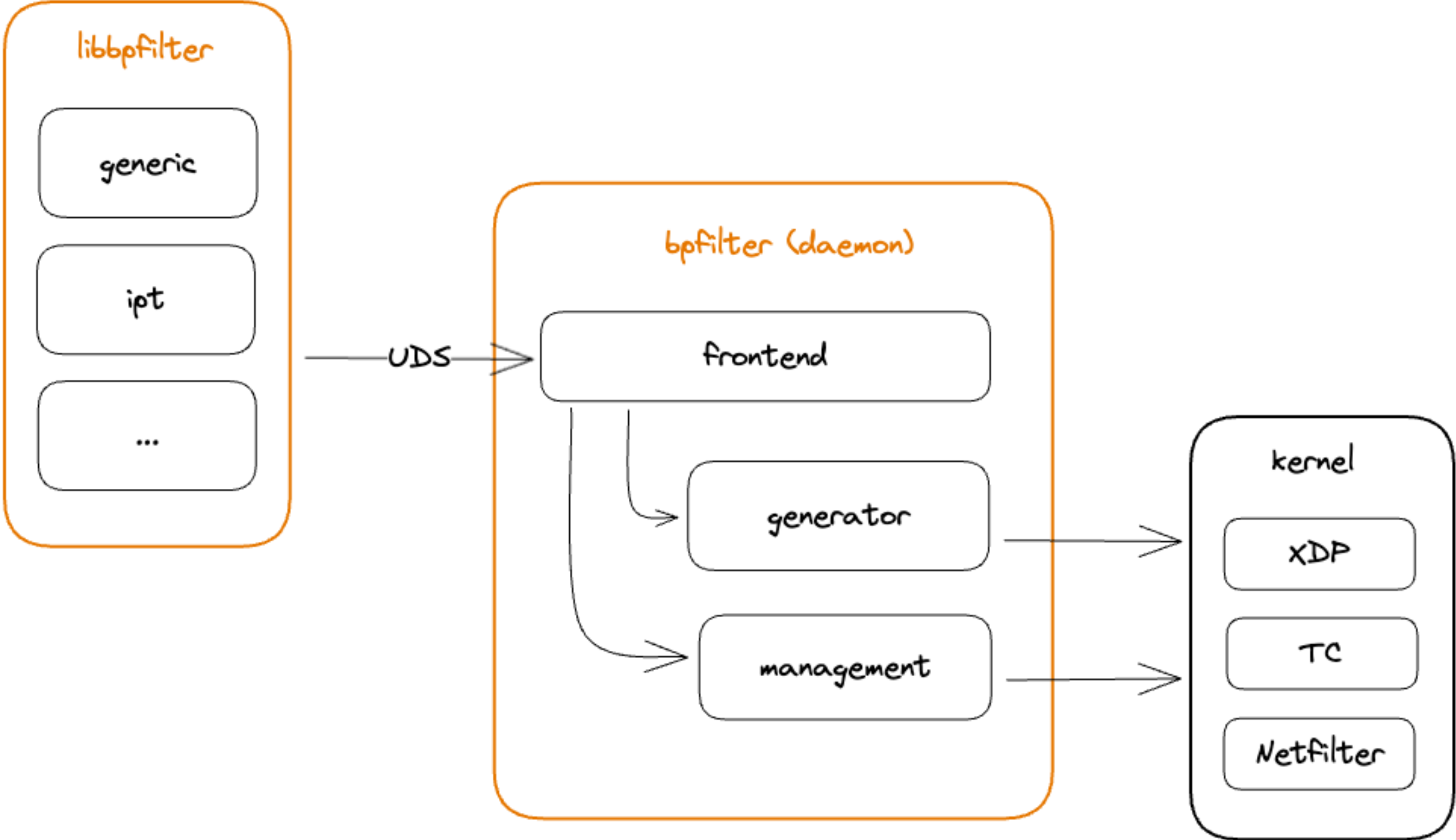
No packages published
[Publish your first package](#)

Languages

C 98.9% Other 1.1%



04 MORE IN DEEP



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

