Nftables Netlink API

NFWS 2017 - Faro, Portugal

Pablo Neira Ayuso <pablo@netfilter.org>

Chain priority order

- Clashing chain priorities: Exposing hook core behaviour, which one comes first?
  - nft add chain x w { … priority 0\; }
  - nft add chain x z { … priority 0\; }
- Solution: Create chain must validate priority too.
  - nft create chain x w { … priority 0\; }
  - nft create chain x z { … priority 0\; }

Chain removal

- chain with rules removal: nft delete chain x y
  - Returns EBUSY
- Inconsistency: Table and set allow removal of populated objects
- Issues:
  - Compatibility layer: non-base removal semantics
  - Reference from another rule via jump...
    - Results in EBUSY