Nftables: What is missing?

Pablo Neira Ayuso
<pablo@netfilter.org>

What is missing?

- Multiple flags inversion, eg. tcp flags != syn,ack
- ICMP codes printing
  - Payload depends on types
  - Offsets overlap
  - rule_print() needs to keep context object around

Need a revisit

- Queue expression
  - U16 for attributes: cannot use 65535 in range, ie. 1-65535 breaks.
- Merge adjacent IPv6 address
  - Two 128 bits
- Connlimit
  - Add translation
- Concatenation: More than 4 commponents in tuple?

Enhancements for expressions

- Enhance extension header
  - Support for SCTP chunk matching
  - Support for DCCP options
- Extension header mangling
  - Allow two more parameters through register for length and offset

Missing features (1)

- sk and tproxy
  - Add expressions
- Policy
  - Support only basic stuff
- String expression
  - Allow offset to application payload?

Missing features (2)

- Time match
  - Implement this from userspace daemon?
- SYN proxy
- Recent
  - Make sure we can emulate this with sets and flow tables

Missing features (3)

- Audit
- Secmark
  - Currently broken in tree
- NPT (IPv6 stateless NAT)

Missing features (4)

- LED expression
- Cgroup2
  - Sent patch, no feedback
  - Pass i-node to identify cgroup, instead of path
    - Problems:
      - i-node not unique.
      - Path string limitations
- Ct timeout interface
  - Similar to ct helper
- Rate limits for named objects