# Nftables: What is missing?

Pablo Neira Ayuso
<pablo@netfilter.org>

# What is missing?

- Set inversion, eg. Ip saddr != { 1.1.1.1, 2.2.2.2}
  - Arturo already sent patches for libnftnl and kernel
  - Missing nft support
- Multiple flags inversion, eg. tcp flags != syn,ack
  - Sent feedback to Laura on this
- ICMP codes printing
  - Payload depends on types
  - Offsets overlap
  - rule_print() needs to keep context object around

# Need a revisit

- Queue expression
  - No map support: Add support for source register
  - U16 for attributes: cannot use 65535 in range, ie. 1-65535 breaks.
- Packet priority handle
  - Broken scanner
  - Fix result in overlap between IPv6 and priority
- Mangling of non-8 bits bound fields
- Merge adjacent Ipv6 address
  - Two 128 bits
- Connlimit
- Concatenation: More than 4 commponents in tuple

# Syntax inconsistencies

- In NAT statements:
  - Missing semicolon in ports
    - … masquerade to :1024-2048
    - … redirect to 1024-2048 (missing semicolon)
  - Missing to in snat and dnat
    - … snat 1.2.3.4 (missing to)
- nft export json
  - Missing object, should be: nft export ruleset json

# Enhancements for expressions

- Enhance extension header
  - Support for TCP options, SCTP
- 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
- Jhash expression
  - To emulte cluster match/CLUSTERIP target.
  - Load balancing: HMARK
- String expression
  - Allow offset to application payload?

# Missing features (2)

- Time match
  - Implement this from userspace daemon?
- Nth match
  - Laura working on this
- Rerverse path filtering
- SYN proxy
- Recent & hashlimit
  - Make sure we can emulate this with sets and flow tables

# Missing features (3)

- Audit
- Secmark
  - Currently broken in tree
- Nfacct
  - Already posted a patchset
  - Still spinning on better integration for named stateful objects.
- NPT (IPv6 stateless NAT)
- Checksum expression
- Addrtype match

# Missing features (4)

- CT template
  - Set helper
- LED expression
- Cgroup2
  - Use immediate to path
- Quota expression
  - Counter expression per-cpu
  - Set infrastructure allow s to attach one expression to element
  - Easy to implement as a standalone expression