ipset status

József Kadlecsik
<kadlec@blackhole.kfki.hu>
KFKI RMKI

ipset in kernel

- ipset v6.0: submitted at 2.6.39
- ipset v6.8: in 3.1

Changes since v6.0

- Bugfixes :-)
  - testsuite
- SCTP, UDPLITE support
- Timeout can be modified for already added elements
- Support listing setnames and headers too
- Support set types with multiple revisions

Changes since v6.0, cont.

- Support range syntax for IPv4 at adding/deleting elements for hash:*net* types: range is converted to the networks equal to the range
- hash:net,iface type introduced

Possible extensions I.

- tc filter support via iptables/ip6tables match support in tc (Jan's idea)
  - tc supports only iptables targets

Possible extensions II.

- ipset state replication support via full iptables/ip6tables match/target state support in conntrack-tools

Possible extensions III.

- Match support in SET target to jump to different decision branches for hash:*net* types
  - Store accept/drop flag in the element

```
ipset new foo hash:net
ipset add foo 192.168.1.1 --drop
ipset add foo 192.168.1.0/24 [--accept]
iptables -A ....
     -j SET --match-set foo dir \
     --match-accept chain1
     --match-drop chain2
```

Performance testing I.

- Requires lot of good hardware
  - ~50 4CPU machines
  - 10Gb interfaces in firewall machine
  - Switches

Performance testing II.

- … and time
  - One single test takes 5minutes, 20 tests in case, repeated 3 times
  - Tested cases:
    - 3 different data sizes: << MTU, = MTU, >> MTU
    - 2 MTUs: normal, jumbo frames
    - INET: IPv4, IPv6
    - Modes: route, stateless iptables, stateless ipset, stateful iptables, stateful ipset, NAT iptables, NAT ipset
  - 5min*20*3*3*2*2*7 ~ 18 days