Ipset status report

József Kadlecsik

New features

- **tc** supports matching in sets, thanks to Florian Westphal
- Range notation for IPv4, ports
- Exceptions in hash:*net* types (“nomatch”)

Packet, byte counters I.

- Fairly larger rewriting:
  - Set element
  - Extensions:
    - Timeout
    - Packet, byte counters

Packet, byte counters II.

- Syntax at ipset:

```
ipset add <set> <elem> packets n bytes m
```

Packet, byte counters III.

- Syntax at iptables:

```
-m set --match-set <set> dir,[...] \
    [! --update-counters] \
    [[!] --packets-eq value |
     --packets-lt value | \
     --packets-gt value ] \
   [[!] --bytes-eq value |
     --bytes-lt value ...]
```

Packet, byte counters IV.

- What if the set is a list of sets: should the counters be updated at the top level only or in the element set too?

```
-m set --match-set <set> dir,[...] \
    [! --update-counters] \
    [! --update-sub-counters] \
    ...
```

Ideas

- Iptables targets as extensions
  - Dependency on iptables
- Generic hash type:
  - ip, port, mac, mark, secmark, uid
- Events:
  - Add, del element
  - Match element?