nftables: the New Fangled (ip)Tables

(but actually netfilter tables)

Charlie Li

PLUG North
13 December 2016

```
iptables -I input -p tcp --dport
80 -m state --state NEW -m
hashlimit --hashlimit-above
20/sec --hashlimit-mode srcip
--hashlimit-name http -j DROP
```

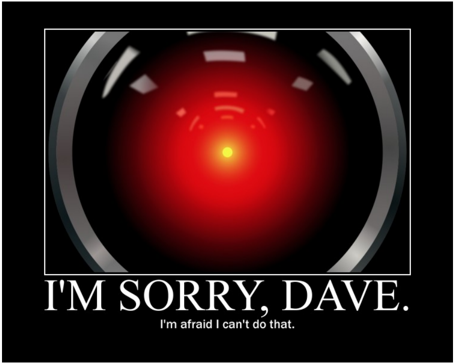
Why nftables?

ie motivation, from both maintainer and user points of view

Why nftables?

ie motivation, from both maintainer and user points of view

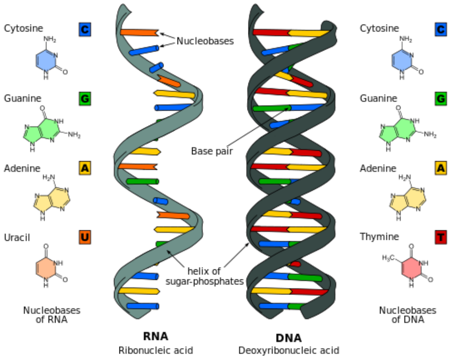
- iptables is old, but more importantly cumbersome af
  - Fifteen tender years
  - Code duplication and inconsistencies: protocol specificities
- Generic, easily extensible architecture
  - Sets, maps
  - Unified dual-stack classification
  - Netlink API
- A real syntax language!



Main differences with iptables

Main differences with iptables

- Syntax
- Fully-configurable tables and chains
- Linear (for now) evaluation of expressions
- Several actions in one rule allowed
- Counters optional
- Better dynamic updates
- Unified dual-stack administration
- Set and map data structures
- Concatenations
- Updates without updating kernel



Availability

because nobody actually bothers to publicise this either

Availability

because nobody actually bothers to publicise this either

Kernel

- Mainlined in 3.13
- Backported to 3.10 used in RHEL/CentOS 7
    - possibly also other enterprise/super stable distro kernels

Availability

because nobody actually bothers to publicise this either

Kernel

- Mainlined in 3.13
- Backported to 3.10 used in RHEL/CentOS 7
  - possibly also other enterprise/super stable distro kernels

Userspace

- `nft` — note one userspace program, compared to at least four!
- `libmnl` — Netlink API
- `libnftnl` — nftables API

Availability

because nobody actually bothers to publicise this either

Kernel

- Mainlined in 3.13
- Backported to 3.10 used in RHEL/CentOS 7
  - possibly also other enterprise/super stable distro kernels

Userspace

- `nft` — note one userspace program, compared to at least four!
- `libmnl` — Netlink API
- `libnftnl` — nftables API

This is usually part of a unified `nftables` package or collection of dependencies

Demo time!