Netfilter software @ Debian

Netfilter Workshop 2018 @ Berlin
Arturo Borrero Gonzalez <arturo@netfilter.og>

Some years ago…

- several Debian Developers involved
- packages in mostly good shape

- previous to the nftables times

Some years ago...

- Then about 2013-2014 all changed
- Most of the developers stopped working

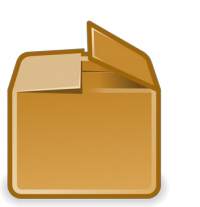
- I took maintenance of many packages [mostly forced]

Big plan: xtables to nftables

- iptables is installed by default in Debian
- Rename binary to **iptables-legacy**
- use iptables-compat transparently if possible
- In the long term: install nftables by default

Big plan: xtables to nftables

- Right now: 3 main packages



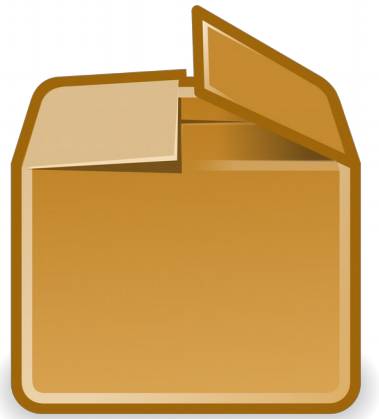
iptables

iptables-nftables-compat

nftables

Big plan: xtables to nftables

iptables contains:

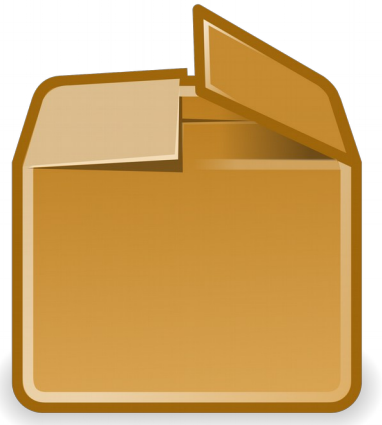


- /sbin/iptables (-restore, -save)
- /sbin/ip6tables (“”)
- extensions

Soon /sbin/iptables-legacy !

Big plan: xtables to nftables

- Iptables-nftables-compat contains:



- Translate tools (/sbin/iptables-translate)
- Compat tools (/sbin/iptables-compat-translate and friends)
- translate/compat extensions for [arp,eb]tables

Soon /sbin/iptables ---(link)---> /sbin/iptables-compat

Big plan: xtables to nftables

- Some tests already succeeded
- libvirt / kvm virtualization live demo

```
table ip mangle {
        chain PREROUTING {
                type filter hook prerouting priority -150; policy accept;
        }

        chain INPUT {
                type filter hook input priority -150; policy accept;
        }

        chain FORWARD {
                type filter hook forward priority -150; policy accept;
        }

        chain OUTPUT {
                type route hook output priority -150; policy accept;
        }

        chain POSTROUTING {
                type filter hook postrouting priority -150; policy accept;
                oifname "virbr0" ip protocol udp udp dport 68 counter packets 2 bytes 656 # CHECKSUM fill
```

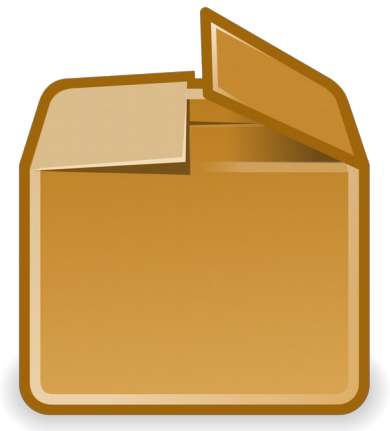
Big plan: xtables to nftables

- Debian’s native `update-alternatives` mechanism (opt-in)

- Allows users to move back and forth the link between -legacy and -compat

arptables & ebtables

- Leftover packages in Debian
- Alberto Molina is helping from Spain



Soon /sbin/arptables-legacy
and /sbin/ebtables-legacy !

Long term future

- Simple goal: use nftables by default
- How will community react to these changes?

Pending work …

- What about ipset-compat?
- Document all these changes
- Coordinate with RedHat & ArchLinux folks
- Missing translations