Xtables2: Packet Filter Evolved

Jan Engelhardt <jan@inai.de>

2013-Mar-10

Xtables

- collective term for iptables, ip6tables, arptables, ebtables (based upon `x_tables.c`)

History time

iptables shortfalls:

- family specific
- duplicated execution logic
- socket protocol that is static by today's means
- etc.

Xtables2
an ongoing effort to evolve the packet filter.

1

[1] http://lwn.net/Articles/345486/

Comparison

A look at some capabilities.

- rule packing
- family independent
- xt extension support
- atomic replace support
- network namespaces
- more...

Backwards compatibility?

- xt extension C code is reused
- iptables's libxtables C code is reused
- command-line syntax: not the same, but very close. The only user visible change, and a justfiable one. The old junk needs to move out, but don't throw everything overboard.

And in the unlikely case:

- I still have the binary compatibility code... (xt2 with iptables frontend)

Read Me

What you get

- Netlink-based interface (xtnl), has had actual developer discussion
- Userspace:
- low-level library for xtnl operations (libnetfilter_xtables)
- high-level library for ruleset inspection/manipulation (libxtadm) (use this for programming and language bindings!)
- Documentation

and that is why you should choose it.

- `http://xtables.de/`