

**NAME**

xtables-legacy — iptables using old getsockopt/setsockopt-based kernel api

**DESCRIPTION**

**xtables-legacy** are the original versions of iptables that use old getsockopt/setsockopt-based kernel interface. This kernel interface has some limitations, therefore iptables can also be used with the newer nf\_tables based API. See **xtables-nft(8)** for information about the xtables-nft variants of iptables.

**USAGE**

The xtables-legacy-multi binary can be linked to the traditional names:

```
/sbin/iptables -> /sbin/iptables-legacy-multi
/sbin/ip6tables -> /sbin/ip6tables-legacy-multi
/sbin/iptables-save -> /sbin/ip6tables-legacy-multi
/sbin/iptables-restore -> /sbin/ip6tables-legacy-multi
```

The iptables version string will indicate whether the legacy API (get/setsockopt) or the new nf\_tables API is used:

```
iptables -V
iptables v1.7 (legacy)
```

**LIMITATIONS**

When inserting a rule using iptables -A or iptables -I, iptables first needs to retrieve the current active rule-set, change it to include the new rule, and then commit back the result. This means that if two instances of iptables are running concurrently, one of the updates might be lost. This can be worked around partially with the --wait option.

There is also no method to monitor changes to the ruleset, except periodically calling iptables-legacy-save and checking for any differences in output.

**xtables-monitor(8)** will need the **xtables-nft(8)** versions to work, it cannot display changes made using the **iptables-legacy** tools.

**SEE ALSO**

**xtables-nft(8)**, **xtables-translate(8)**

**AUTHORS**

Rusty Russell originally wrote iptables, in early consultation with Michael Neuling.