

---

Subject: Re: [PATCH] NETFILTER: per-netns FILTER/MANGLE/RAW tables for real

Posted by [Patrick McHardy](#) on Thu, 20 Mar 2008 15:29:42 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Alexey Dobriyan wrote:

- > Commit 9335f047fe61587ec82ff12fbb1220bcfdd32006 aka
- > "[NETFILTER]: ip\_tables: per-netns FILTER, MANGLE, RAW"
- > added per-netns `_view_` of iptables rules. They were shown to user, but
- > ignored by filtering code. Now that it's possible to at least ping loopback,
- > per-netns tables can affect filtering decisions.
- >
- > netns is taken in case of
- > `PRE_ROUTING`, `LOCAL_IN` -- from in device,
- > `POST_ROUTING`, `LOCAL_OUT` -- from out device,
- > `FORWARD` -- from in device which should be equal to out device's netns.
- > This code is relatively new, so `BUG_ON` was plugged.
- >
- > Wrappers were added to a) keep code the same from `CONFIG_NET_NS=n` users
- > (overwhelming majority), b) consolidate code in one place -- similar
- > changes will be done in ipv6 and arp netfilter code.

Applied, thanks.

---