

Re: [PATCH] ng\_tag – new netgraph node, please test (L7 filtering possibility)

## Re: [PATCH] ng\_tag – new netgraph node, please test (L7 filtering possibility)

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/isp/2006-06/msg00044.html>

---

- *From:* "Vadim Goncharov" <[vadim\\_nuclight@xxxxxxx](mailto:vadim_nuclight@xxxxxxx)>
  - *Date:* Mon, 12 Jun 2006 03:19:44 +0700
- 

11.06.06 @ 22:36 Joao Barros wrote:

Original message is at: <http://lists.freebsd.org/pipermail/freebsd-current/2006-June/063821.html>

I'm very interested in this, great work! :-)  
I can't load the kld on my Sun Sparc, I think I messed up ld yesterday trying to patch for a bug that show's in firefox and mozilla. It compiles, just doesn't run. As soon as I have it up and running I'll give you feedback.

Umm, that's a kernel module, it shouldn't have any relations with ld. What diagnostics has it said on failed load?

Have you tested it with pf? If so can you give me some examples?

No, it wasn't tested with pf. The problem with pf is that pf compiles all the rules at the time, so exact tags representation can change each time (for this reason ipfw tags were made incompatible with pf), and you must that values to supply them to . However, if you find a method how to obtain tag values info from in-kernel pf structures, you'll be able to use it with pf. It doesn't support well integration with netgraph, though.

Another option is to use ipfw – it supports pf's altq(4) shaping, if that is all you need.

I'm particularly interested in this for doing packed shaping, especially on P2P.

Yes, I'm also looking for possibility of shaping, but I can't test (no resources) it currently. Also, as it seems non-trivial on current ipfw dynamic rules implementation, I don't know if shaping will work at all.

But you can try to test such ruleset (it supposes that dynamic rules are checked twice, on incoming packets and on outgoing also, as with all other rules as ipfw manpage says):

```
# first, split traffic to incoming to our router and outgoing
ipfw add 100 skipto 600 ip from any to any out
```

Re: [PATCH] ng\_tag – new netgraph node, please test (L7 filtering possibility)

Re: [PATCH] ng\_tag – new netgraph node, please test (L7 filtering possibility)

```
# check-state for incoming packets will catch all already matched
# p2p connections, and continue to "tag 412" rest of them
ipfw add 200 check-state

# pass yet unrecognized incoming traffic to netgraph for analyzing
# note that only one packet for connection will be tagged, not others
# in the flow!
ipfw add 300 netgraph 41 ip from any to any # XXX more limits?

# let's create a state dynamic rule after one tagged packet – dynamic
# rules only match addresses and ports, and then use parent rule to
# determine action, and will also "tag 412" for every next packet
# in that connection, so that's the way how we can catch packets on output
# from our router
ipfw add 400 pass tag 412 ip from any to any tagged 412 keep-state

# this is the point where all other unmatched incoming traffic goes so
# it must caught here or it will be matched for next rule, but next rule
# should match outgoing traffic only
ipfw add 500 pass ip from any to any

# here is output were all packets which belong to p2p connections are
# tagged 412 by dynamic rules, so we can send them all to pipe (or you
# can use altq(4) here, of course).. the only thing to note that packets
# to both directions of our router are sent to only one pipe, but for
# my example it's enough
ipfw add 600 pipe 40 ip from any to any tagged 412
```

--

WBR, Vadim Goncharov

---

freebsd-isp@xxxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-isp>

To unsubscribe, send any mail to "freebsd-isp-unsubscribe@xxxxxxxxxxxxx"