Packet flow in Netfilter and General Networking

Other NF parts
Other Networking

basic set of filtering
opportunities at the

network level
bridge level

INPUT PATH **FORWARD PATH** **OUTPUT PATH**

Application Layer

local process

Protocol Layer

by Jan Engelhardt
(based in part on Joshua Snyder's graph)
Last updated 2014-Feb-28; Linux 2.6.36+

clone packet

xfrm (e.g. ipsec) decode

xfrm/socket lookup

no clone to AF_PACKET

xfrm encode

Network Layer

* "security" table left
  out for brevity
* "nat" table only consulted
  for "NEW" connections

filter input

mangle input

routing decision

raw output

conntrack

mangle output

reroute check

filter output

nat output

raw prerouting

conntrack

mangle prerouting

nat prerouting

routing decision

mangle forward

filter forward

mangle postrouting

nat postrouting

xfrm lookup

Link Layer

filter input

mangle forward

filter forward

mangle postrouting

nat postrouting

nat output

filter output

nat postrouting

broute brouting

nat prerouting

raw prerouting

conntrack

mangle prerouting

nat prerouting

bridging decision

filter forward

mangle forward

filter forward

nat postrouting

mangle postrouting

nat postrouting

clone packet

taps (e.g. AF_PACKET)

clone packet

(start)

ingress (qdisc)

bridge check

egress (qdisc)

interface output

AF_PACKET