Linux NetFilter, IP Tables and Conntrack Diagrams

Netfilter-IPTables-Diagrams.md

Linux NetFilter, IP Tables and Conntrack Diagrams

IPTABLES TABLES and CHAINS

IPTables has the following 4 built-in tables.

1) Filter Table

Filter is default table for iptables. So, if you don't define you own table, you'll be using filter table. Iptables's filter table has the following built-in chains.

- INPUT chain – Incoming to firewall. For packets coming to the local server.
- OUTPUT chain – Outgoing from firewall. For packets generated locally and going out of the local server.
- FORWARD chain – Packet for another NIC on the local server. For packets routed through the local server.

2) NAT table

Iptable's NAT table has the following built-in chains.

- PREROUTING chain – Alters packets before routing. i.e Packet translation happens immediately after the packet comes to the system (and before routing). This helps to translate the destination ip address of the packets to something that matches the routing on the local server. This is used for DNAT (destination NAT).
- POSTROUTING chain – Alters packets after routing. i.e Packet translation happens when the packets are leaving the system. This helps to translate the source ip address of the packets to something that might match the routing on the desintation server. This is used for SNAT (source NAT).
- OUTPUT chain – NAT for locally generated packets on the firewall.

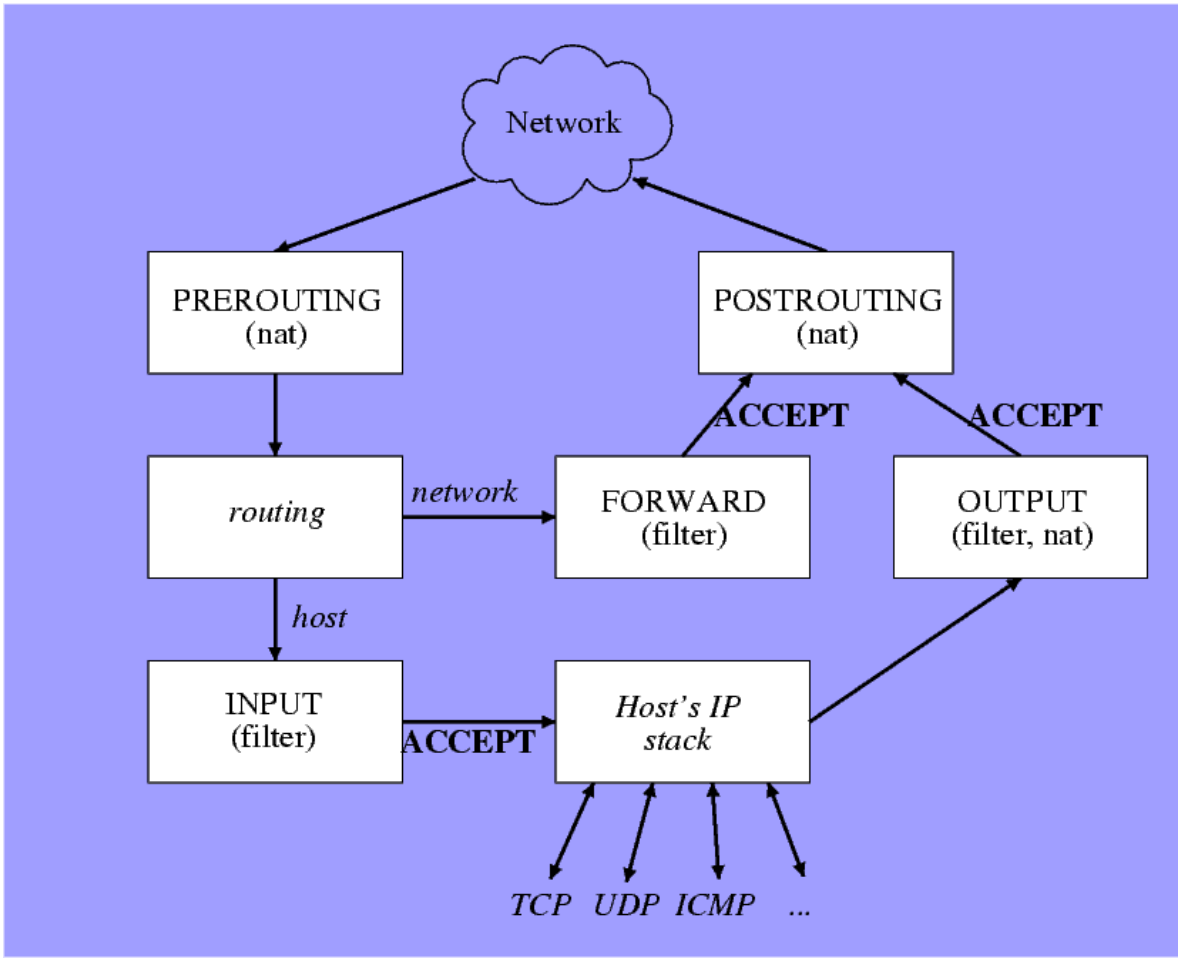
3) Mangle table

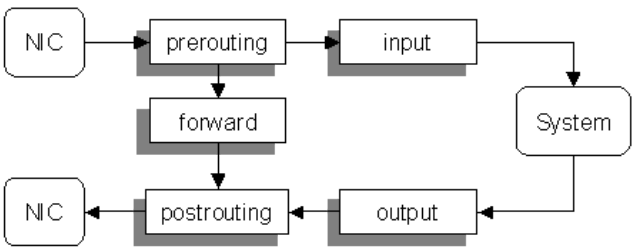
Iptables's Mangle table is for specialized packet alteration. This alters QOS bits in the TCP header. Mangle table has the following built-in chains.

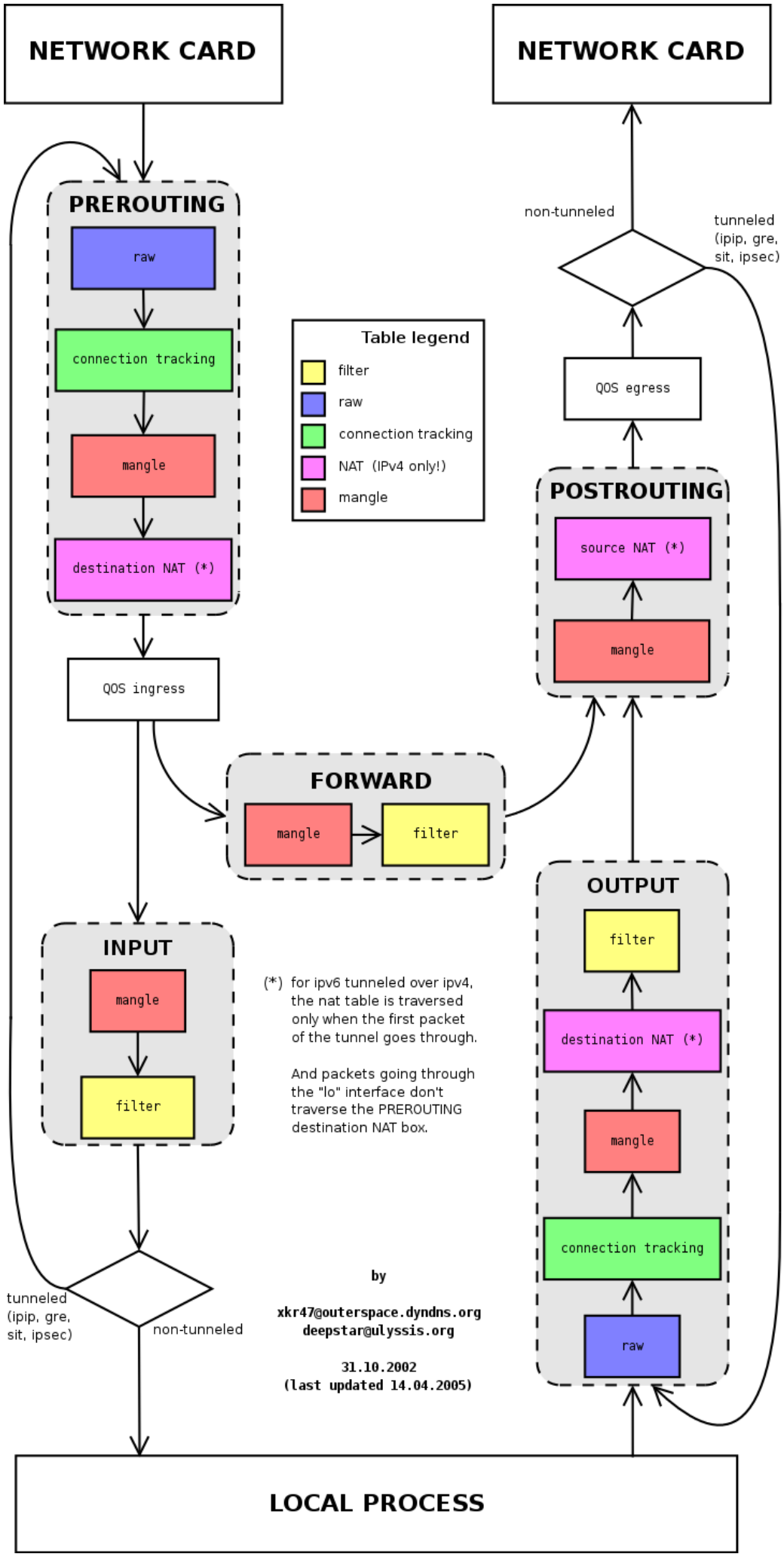
- PREROUTING chain
- OUTPUT chain
- FORWARD chain
- INPUT chain
- POSTROUTING chain

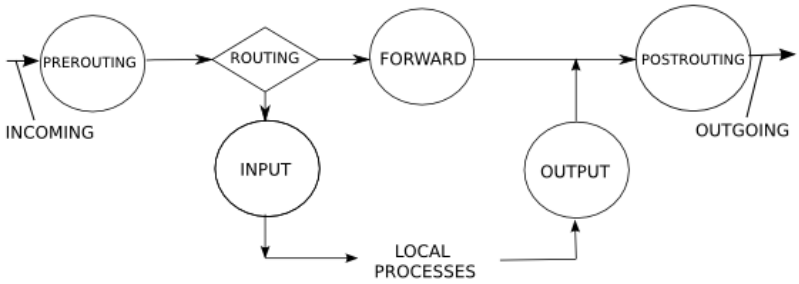
4) Raw table

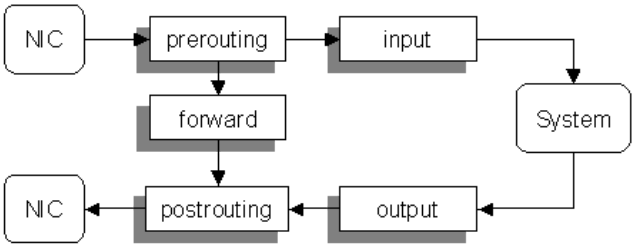
Iptable's Raw table is for configuration exemptions. Raw table has the following built-in chains.

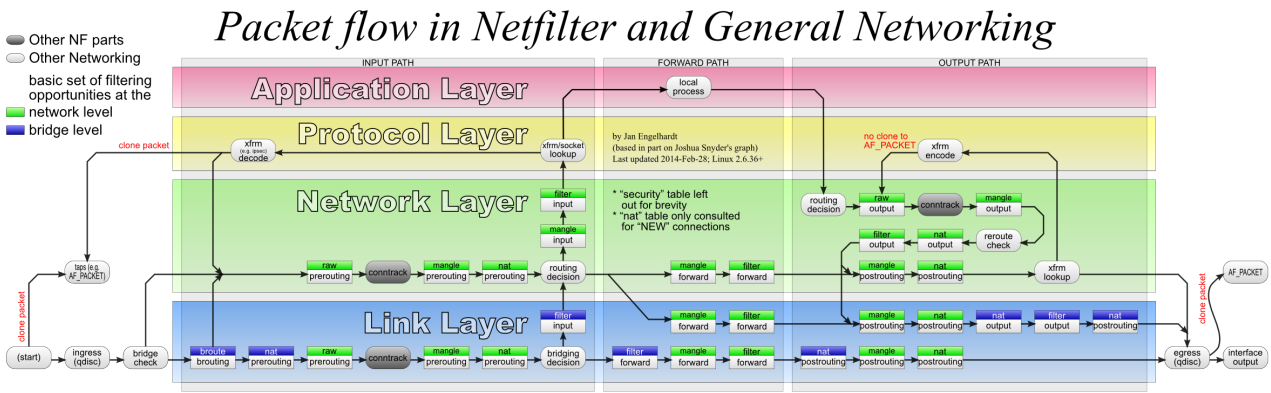

Network
PREROUTING
(nat)
POSTROUTING
(nat)
ACCEPT
ACCEPT
routing
network
FORWARD
(filter)
OUTPUT
(filter, nat)
host
INPUT
(filter)
ACCEPT
Host's IP
stack
TCP
UDP
ICMP
...

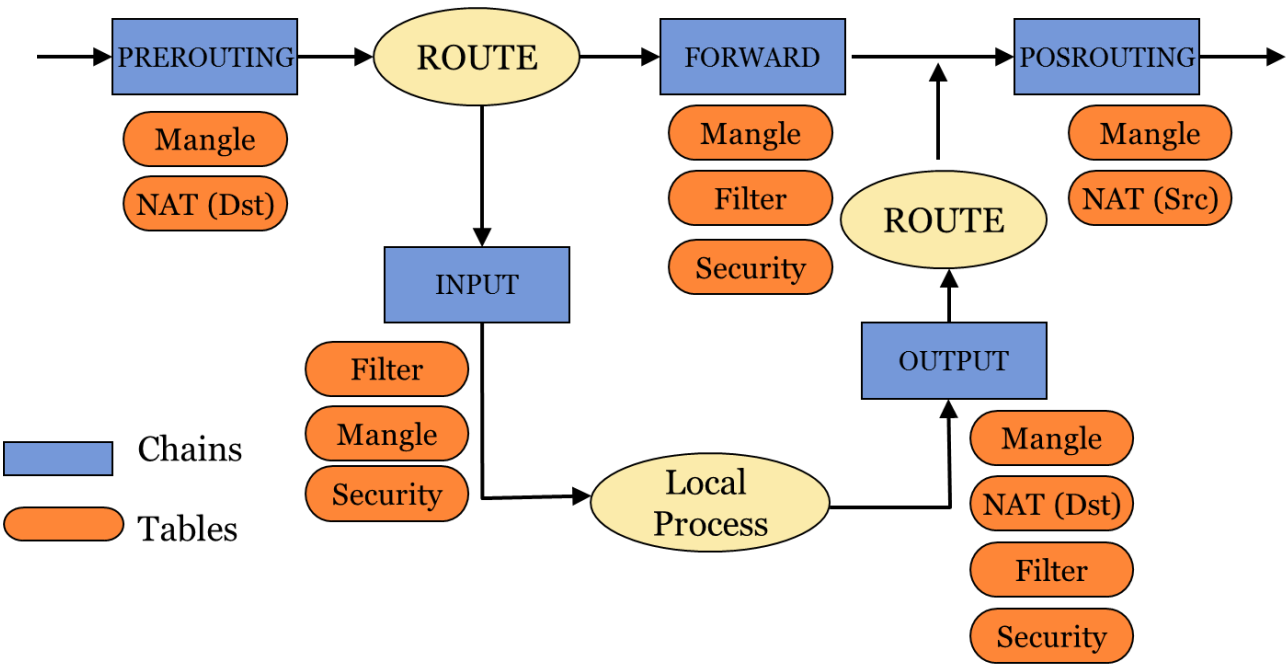

NIC
prerouting
input
forward
System
NIC
postrouting
output

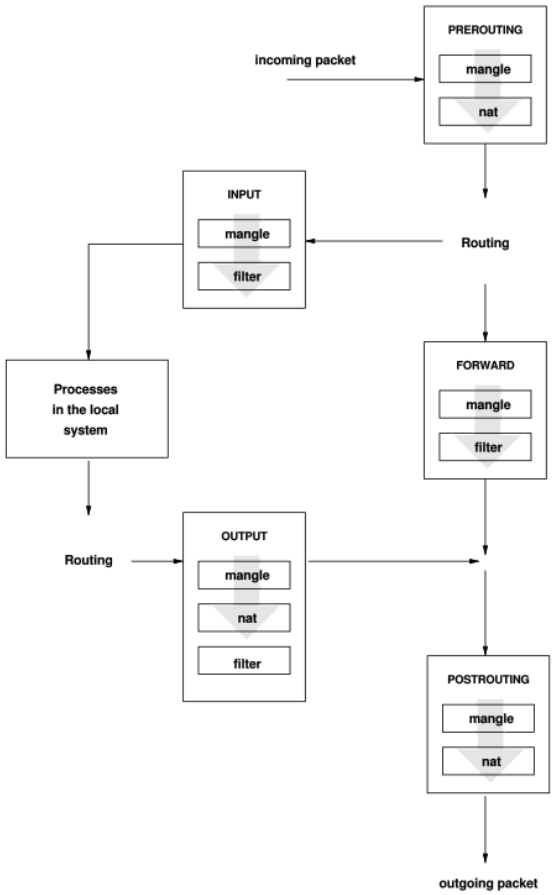

NETWORK CARD
NETWORK CARD
PREROUTING
raw
connection tracking
mangle
destination NAT (*)
QOS ingress
Table legend
filter
raw
connection tracking
NAT (IPv4 only!)
mangle
non-tunneled
tunneled
(ipip, gre,
sit, ipsec)
QOS egress
POSTROUTING
source NAT (*)
mangle
FORWARD
mangle
filter
INPUT
mangle
filter
OUTPUT
filter
destination NAT (*)
mangle
connection tracking
raw
(*) for ipv6 tunneled over ipv4,
the nat table is traversed
only when the first packet
of the tunnel goes through.
And packets going through
the "lo" interface don't
traverse the PREROUTING
destination NAT box.
by
xkr47@outerspace.dyndns.org
deepstar@ulyssis.org
31.10.2002
(last updated 14.04.2005)
tunneled
(ipip, gre,
sit, ipsec)
non-tunneled
LOCAL PROCESS

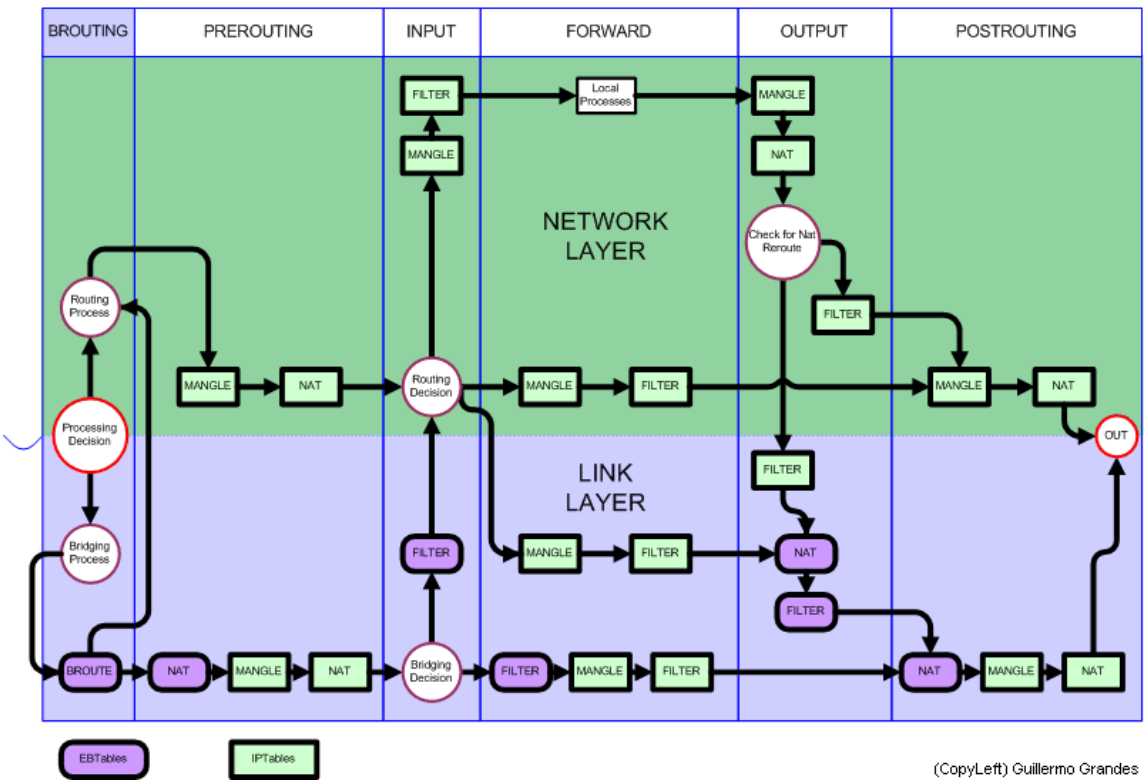

PREROUTING
ROUTING
FORWARD
POSTROUTING
INCOMING
OUTGOING
INPUT
OUTPUT
LOCAL
PROCESSES

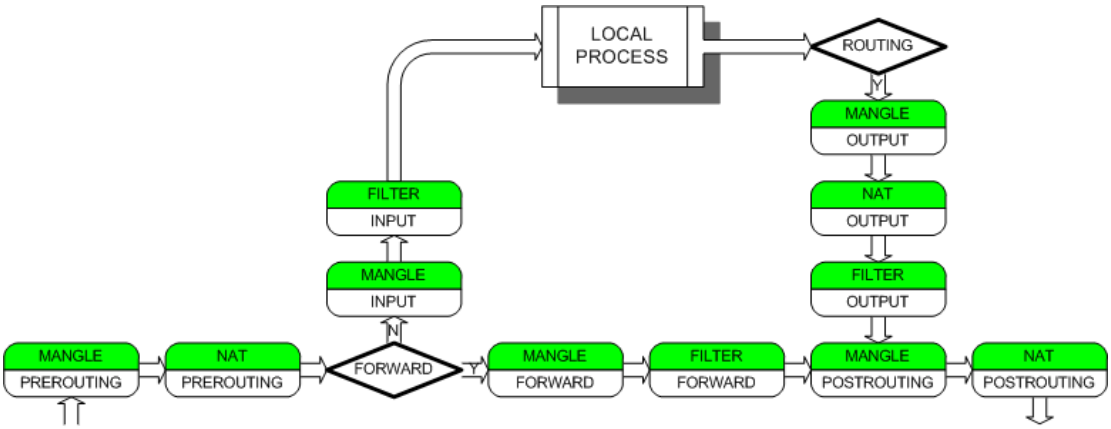

NIC
prerouting
input
forward
System
NIC
postrouting
output

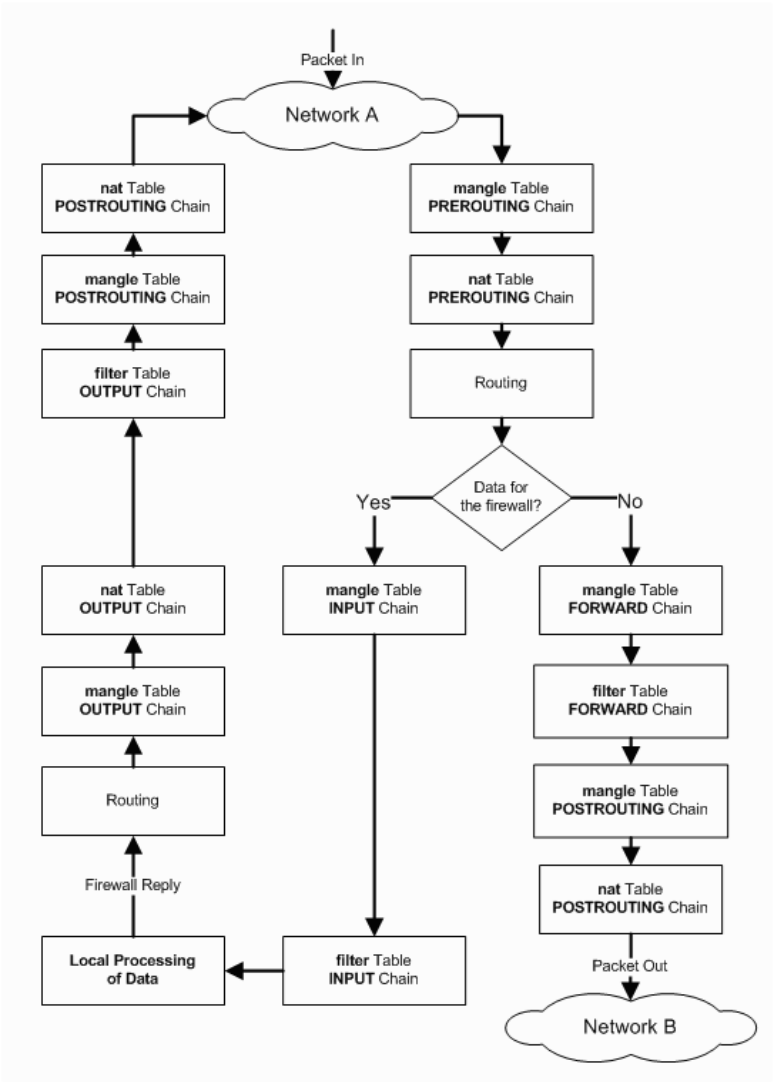

Packet flow in Netfilter and General Networking
Other NF parts
Other Networking
basic set of filtering opportunities at the
network level
bridge level
INPUT PATH
FORWARD PATH
OUTPUT PATH
Application Layer
Protocol Layer
Network Layer
Link Layer
local process
by Jan Engelhardt
(based in part on Joshua Snyder's graph)
Last updated 2014-Feb-28; Linux 2.6.36+
* "security" table left out for brevity
* "nat" table only consulted for "NEW" connections
clone packet
no clone to AF_PACKET
(start)
ingress (qdisc)
bridge check
routing decision
bridging decision
egress (qdisc)
interface output
AF_PACKET

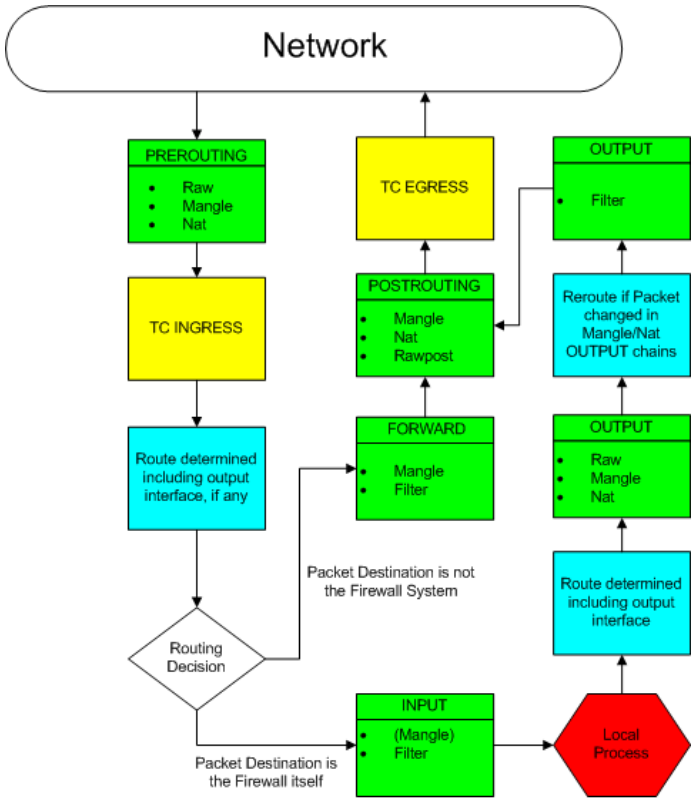

PREROUTING
ROUTE
FORWARD
POSROUTING
Mangle
NAT (Dst)
Mangle
Filter
Security
Mangle
NAT (Src)
ROUTE
INPUT
OUTPUT
Filter
Mangle
Security
Local Process
Mangle
NAT (Dst)
Filter
Security
Chains
Tables


incoming packet
PREROUTING
mangle
nat
INPUT
mangle
filter
Routing
Processes in the local system
FORWARD
mangle
filter
Routing
OUTPUT
mangle
nat
filter
POSTROUTING
mangle
nat
outgoing packet

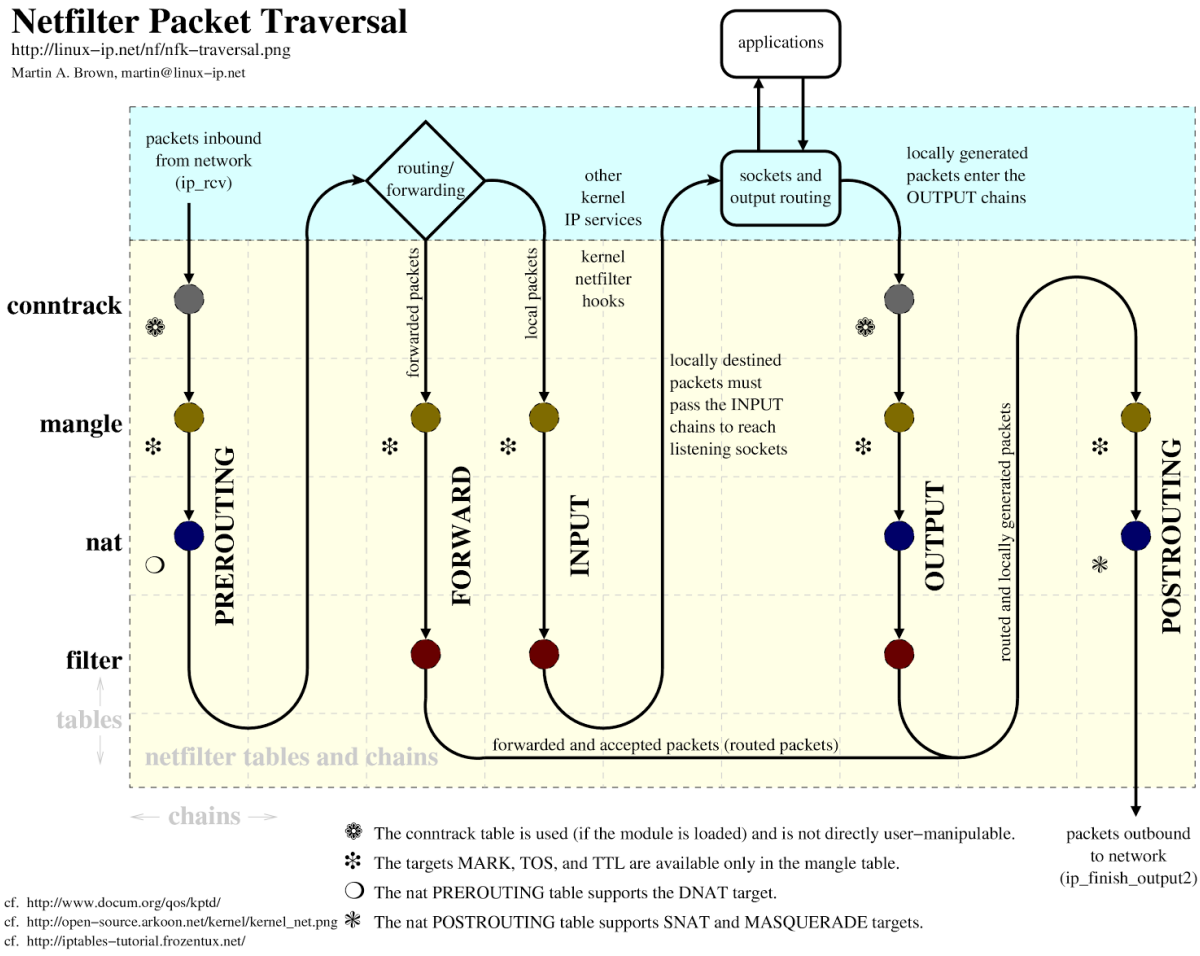

BROUTING
PREROUTING
INPUT
FORWARD
OUTPUT
POSTROUTING
NETWORK LAYER
LINK LAYER
Routing Process
Processing Decision
Bridging Process
BROUTE
NAT
MANGLE
FILTER
Routing Decision
Bridging Decision
Local Processes
Check for Nat Reroute
OUT
EBTables
IPTables
(CopyLeft) Guillermo Grandes


LOCAL PROCESS
ROUTING
MANGLE
OUTPUT
NAT
OUTPUT
FILTER
OUTPUT
FILTER
INPUT
MANGLE
INPUT
N
MANGLE
PREROUTING
NAT
PREROUTING
FORWARD
Y
MANGLE
FORWARD
FILTER
FORWARD
MANGLE
POSTROUTING
NAT
POSTROUTING


Packet In
Network A
nat Table
POSTROUTING Chain
mangle Table
POSTROUTING Chain
filter Table
OUTPUT Chain
mangle Table
PREROUTING Chain
nat Table
PREROUTING Chain
Routing
Data for
the firewall?
Yes
No
nat Table
OUTPUT Chain
mangle Table
OUTPUT Chain
Routing
Firewall Reply
Local Processing
of Data
mangle Table
INPUT Chain
filter Table
INPUT Chain
mangle Table
FORWARD Chain
filter Table
FORWARD Chain
mangle Table
POSTROUTING Chain
nat Table
POSTROUTING Chain
Packet Out
Network B



Netfilter Packet Flow



anudeep404 commented on 11 May 2018

If we were to configure IPSec VPN with openswan, how does it pass through these chains?

ArthurChiao commented on 28 Jan 2019

nice!

sliddjur commented on 24 Oct 2019 • edited

> If we were to configure IPSec VPN with openswan, how does it pass through these chains?

I think like this https://gist.github.com/nerdalert/a1687ae4da1cc44a437d#-2 ? **@anudeep404**