PF\_INET的netfilter

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | NF\_IP\_PRE\_ROUTING  ip\_rcv()中调用 | NF\_IP\_LOCAL\_IN  ip\_local\_deliver() | NF\_IP\_FORWARD  ip\_forward() | NF\_IP\_LOCAL\_OUT  ip\_queue\_xmit()  ip\_push\_pending\_frames  raw\_send\_hdrinc | NF\_IP\_POST\_ROUTING  ip\_mc\_output  ip\_output  xfrm4\_output |
| NF\_IP\_PRI\_FIRST | ip\_sabotage\_in |  |  |  |  |
| -400 NF\_IP\_PRI\_CONNTRACK\_DEFRAG | ipv4\_conntrack\_defrag |  |  | ipv4\_conntrack\_defrag |  |
| -300 NF\_IP\_PRI\_RAW | ipt\_hook |  |  | ipt\_local\_hook |  |
| -200 NF\_IP\_PRI\_CONNTRACK | ipv4\_conntrack\_in |  |  | ipv4\_conntrack\_local |  |
| -150 NF\_IP\_PRI\_MANGLE | ipt\_route\_hook | ipt\_route\_hook | ipt\_route\_hook | ipt\_local\_hook | ipt\_route\_hook |
| -100 NF\_IP\_PRI\_NAT\_DST | nf\_nat\_in |  |  | nf\_nat\_local\_fn |  |
| 0 NF\_IP\_PRI\_FILTER |  | ipt\_hook | ipt\_hook | ipt\_local\_out\_hook |  |
| 100 NF\_IP\_PRI\_NAT\_SRC |  | nf\_nat\_fn |  |  | nf\_nat\_out |
| 225 NF\_IP\_PRI\_SELINUX\_LAST | selinux\_ipv4\_postroute\_last |  |  |  |  |
| INT\_MAX – 2 NF\_IP\_PRI\_CONNTRACK\_HELPER |  | ipv4\_conntrack\_help |  |  | ipv4\_conntrack\_help |
| INT\_MAX – 1  NF\_IP\_PRI\_NAT\_SEQ\_ADJUST |  | nf\_nat\_adjust |  |  | nf\_nat\_adjust |
| NF\_IP\_PRI\_CONNTRACK\_CONFIRM |  | ipv4\_confirm |  |  | ipv4\_confirm |
| NF\_IP\_PRI\_LAST |  |  |  |  |  |

数据包的流向无非三种：

发给本地(网关)的数据包：流程PRE\_ROUTING->LOCAL\_IN；

经过本地的数据包（转发包），流程是PRE\_ROUTING->FORWARD->POST\_ROUTING；

从本地(网关)发出的数据包，流程是LOCAL\_OUT->POST\_ROUTING。

发给本地进程 ipv4\_conntrack\_defrag --> ipv4\_conntrack\_in --> ipv4\_confirm

转发数据 ipv4\_conntrack\_defrag --> ipv4\_conntrack\_local –> ipv4\_confirm

发出的数据 ipv4\_conntrack\_defrag --> nf\_conntrack\_in—> ipv4\_confirm