## **Netfilter Packet Traversal** applications http://linux-ip.net/nf/nfk-traversal.png Martin A. Brown, martin@linux-ip.net packets inbound locally generated from network routing/ other sockets and packets enter the (ip\_rcv) forwarding output routing **OUTPUT** chains kernel IP services local packets forwarded packets kernel netfilter hooks conntrack locally destined packets must pass the INPUT couted and locally generated packets mangle chains to reach \* \* \* \* **POSTROUTING** listening sockets PREROUTING FORWARD OUTPUT INPUT nat \*filter tables forwarded and accepted packets (routed packets) netfilter tables and chains chains -> The conntrack table is used (if the module is loaded) and is not directly user-manipulable. packets outbound to network The targets MARK, TOS, and TTL are available only in the mangle table. (ip finish output2) O The nat PREROUTING table supports the DNAT target.

cf. http://www.docum.org/qos/kptd/

cf. http://open-source.arkoon.net/kernel\_net.png \* The nat POSTROUTING table supports SNAT and MASQUERADE targets.

cf. http://iptables-tutorial.frozentux.net/