The Wayback Machine - https://web.archive.org/web/20160101194846/http://netfilter.org/

netfilter
firewalling, NAT, and packet mangling for linux

The netfilter.org project

What is netfilter.org?

netfilter.org is home to the software of the packet filtering framework inside the Linux 2.4.x and later kernel series. Software commonly associated with netfilter.org is iptables.

Software inside this framework enables packet filtering, network address [and port] translation (NA[P]T) and other packet mangling. It is the re-designed and heavily improved successor of the previous Linux 2.2.x ipchains and Linux 2.0.x ipfwadm systems.

netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists of a number of classifiers (iptables matches) and one connected action (iptables target).

netfilter, ip_tables, connection tracking (ip_conntrack, nf_conntrack) and the NAT subsystem together build the major parts of the framework.

Main Features

- stateless packet filtering (IPv4 and IPv6)
- stateful packet filtering (IPv4 and IPv6)
- all kinds of network address and port translation, e.g. NAT/NAPT (IPv4 and IPv6)
- flexible and extensible infrastructure
- multiple layers of API's for 3rd party extensions

What can I do with netfilter/iptables?

- build internet firewalls based on stateless and stateful packet filtering
- deploy highly available stateless and stateful firewall clusters

- use NAT and masquerading for sharing internet access if you don't have enough public IP addresses
- use NAT to implement transparent proxies
- aid the tc and iproute2 systems used to build sophisticated QoS and policy routers
- do further packet manipulation (mangling) like altering the TOS/DSCP/ECN bits of the IP header

Pablo Neira Ayuso