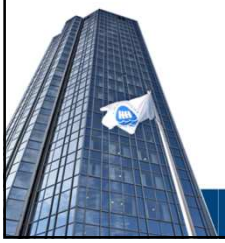
Care and Feed of IP-tables



Mattias Wecksten 2010

iptabels

- Policy
  - Chain
  - Chain
  - Chain
    - Rule
    - Rule
    - Rule

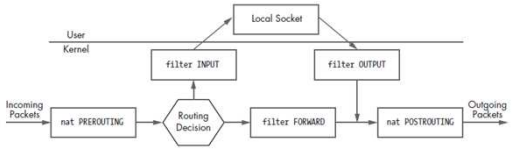
Mattias Wecksten 2010

Tables

- filter
- nat
- mangle
- raw

Mattias Wecksten 2010

Chains



Matches

`--source (-s)`	Match on a source IP address or network
`--destination (-d)`	Match on a destination IP address or network
`--protocol (-p)`	Match on an IP value
`--in-interface (-i)`	Input interface (e.g., eth0)
`--out-interface (-o)`	Output interface
`--state`	Match on a set of connection states
`--string`	Match on a sequence of application layer data bytes
`--comment`	Associate up to 256 bytes of comment data with a rule within kernel memory

Targets

`ACCEPT`	Allows a packet to continue on its way.
`DROP`	Drops a packet. No further processing is performed, and as far as the receiving stack is concerned, it is as though the packet was never sent.
`LOG`	Logs a packet to syslog.
`REJECT`	Drops a packet and simultaneously sends an appropriate response packet (e.g., a TCP Reset packet for a TCP connection or an ICMP Port Unreachable message for a UDP packet).
`RETURN`	Continues processing a packet within the calling chain.

Default IP-tables policy

- DNS
- FTP
- NTP
- SSH
- SMTP
- HTTP/HTTPS
- whois

Assumptions

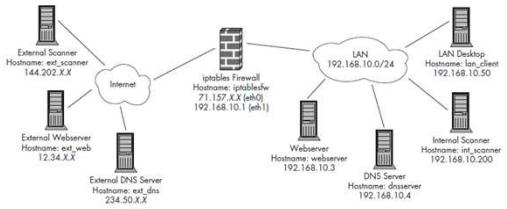


Figure 1-2: Default network diagram

Preamble

INPUT

OUTPUT

FORWARD

NAT

All systems are go

Testing TCP

- nc

Testing UDP

- hping

Testing ICMP

- hping