IPTables

- Available on Linux since 1998
- ipchains (pre-1998)
- Linux Netfilter
- Firewalld, UFW, libvirt, Docker use IPTables; rudimentary support
- IPv6 is an afterthought

```
iptables -P INPUT DROP
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -L INPUT
Chain INPUT (policy DROP)
target prot opt source
                                        destination
ACCEPT all — anywhere
                                        anywhere
                                                            state ESTABLISHED
iptables -I INPUT 1 -m state --state NEW -j ACCEPT
iptables -L INPUT
Chain INPUT (policy DROP)
target prot opt source
                                        destination
ACCEPT all — anywhere
                                        anywhere
                                                            state NEW
ACCEPT
          all — anywhere
                                        anywhere
                                                            state ESTABLISHED
iptables-save | tee rules.persist
*filter
:INPUT DROP [31:7573]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state NEW -j ACCEPT
-A INPUT -m state --state ESTABLISHED -j ACCEPT
COMMIT
iptables -F; iptables -X; iptables-restore < rules.persist
```

NFTables

- Available since Linux 3.13;
 1/19/2014
- 1.0.0 released 8/19/2021
- Linux Netfilter
- IPv4 and IPv6 rules can be mixed or separate (using the meta selectors)
- Can define tables and chains
- Encompasses sets, ebtables, arptables within the language
- Benchmarks: https://developers.redhat.com/blog/2017/04/11/benchmarking-nftables