Key/value maps and verdict maps

- Anonymous maps
- Named maps
- Anonymous vmaps
- Named vmaps

```
nft add chain inet firewall prerouting '{type nat hook prerouting priority 0; policy accept; }'
nft add rule inet firewall prerouting dnat ip to tcp dport map '{ 80: 192.168.1.100, 8888: 192.168.1.101 }'

nft add chain inet firewall postrouting '{type nat hook postrouting priority 0; policy accept; }'
nft add map inet firewall named_map  '{ type inet_service: ipv4_addr; }'
nft add element inet firewall named_map '{ 81: 192.168.1.102, 8080: 192.168.1.103 }'
nft add rule inet firewall postrouting snat ip to tcp dport map @named_map

nft add chain inet firewall icmp-chain
nft add chain inet firewall tcp-chain
nft add chain inet firewall udp-chain
nft add rule inet firewall icmp-chain counter
nft add rule inet firewall tcp-chain counter
nft add rule inet firewall udp-chain counter
nft insert rule inet firewall input handle 7 ip protocol vmap '{ tcp: jump tcp-chain, udp: jump udp-chain, icmp: jump icmp-chain }'

nft add map inet firewall named_vmap '{ type ipv4_addr: verdict; }'
nft add element inet firewall named_vmap '{ 192.168.0.10: drop, 192.168.0.11: accept }'
nft insert rule inet firewall input handle 8 ip saddr vmap @named_vmap
```

Metering and updating sets

```
nft add chain inet firewall incoming_dns

nft add set inet firewall dns_rate_meter '{ type ipv4_addr; size 64; flags timeout, dynamic; }'

nft add rule inet firewall incoming_dns udp dport 53 add @dns_rate_meter '{ ip saddr timeout 60s }' counter accept
nft add rule inet firewall incoming_dns counter log prefix 'dns-rate-meter-breach' group 4 counter drop

nft insert rule inet firewall input handle 5 udp dport 53 jump incoming_dns

sudo python3 -c 'from scapy.all import *; from ipaddress import IPv4Network; [sendp(Ether() / IP(src = str(addr), dst = "192.168.64.5") /
UDP(dport = 53) / DNS(rd = 1, qd = DNSQR(qname = "lame.ddos")), iface = "bridge100") for addr in IPv4Network("192.168.0.0/24").hosts()]'

nft list set inet firewall dns_rate_meter
table inet firewall {
   set dns_rate_meter {
      type ipv4_addr
      size 64
      flags dynamic,timeout
      elements = { 192.168.0.1 timeout 1m expires 57s576ms, 192.168.0.2 timeout 1m expires 57s580ms,
             192.168.0.3 timeout 1m expires 57s588ms, 192.168.0.4 timeout 1m expires 57s592ms,
             192.168.0.5 timeout 1m expires 57s600ms, 192.168.0.6 timeout 1m expires 57s604ms,
             192.168.0.7 timeout 1m expires 57s612ms, 192.168.0.8 timeout 1m expires 57s616ms,
             192.168.0.9 timeout 1m expires 57s624ms, 192.168.0.10 timeout 1m expires 57s628ms,
             …
             192.168.0.63 timeout 1m expires 57s936ms, 192.168.0.64 timeout 1m expires 57s944ms }
   }
}

nft list chain inet firewall incoming_dns
table inet firewall {
   chain incoming_dns {
      udp dport 53 add @dns_rate_meter { ip saddr timeout 1m } counter packets 192 bytes 10560 accept
      counter packets 570 bytes 31350 log prefix "dns-rate-meter-breach" group 4 counter packets 570 bytes 31350 drop
   }
}
```