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

```
nft flush ruleset ; nft add table inet firewall

nft add chain inet firewall input '{ type filter hook input priority filter; policy accept; }'

nft add rule inet firewall input ct state established accept

nft add rule inet firewall input meta nfproto {ipv4, ipv6} tcp dport 22 accept

nft add chain inet firewall input '{ policy drop; }'

nft -a list ruleset | tee nft.conf

table inet firewall { # handle 1
   chain input { # handle 1
      type filter hook input priority filter; policy drop;
      ct state established accept # handle 4
      meta nfproto { ipv4, ipv6 } tcp dport 22 accept # handle 6
   }
}

nft flush ruleset ; nft -f nft.conf
```

https://wiki.nftables.org/wiki-nftables/index.php/Main_Page

https://cloud.ibm.com/docs/vpc?topic=vpc-imd-security-best-practices

Filtering IMDS Access

```
nft add set inet firewall imds_authorized "{ type uid; flags interval; };"
nft add element inet firewall imds_authorized "{ ssm-user }"
nft add chain inet firewall output '{ type filter hook output priority filter; policy accept;}'


nft add rule inet firewall output ip daddr 169.254.0.0/16 skuid @imds_authorized log prefix "imds-authorized" group 2 counter accept

nft add rule inet firewall output ip daddr 169.254.0.0/16 log prefix "imds-unauthorized" group 3 counter drop

tcpdump -vv -n -e -ttt -i nflog:3 -XX
tcpdump: listening on nflog:3, link-type NFLOG (Linux netfilter log messages), snapshot length 262144 bytes
 00:00:00.000000 version 0, resource ID 3, family IPv4 (2), length 148: (tos 0x0, ttl 64, id 43631, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.64.5 > 169.254.169.254: ICMP echo request, id 41821, seq 1, length 64
   0x0000:  0200 0003 0800 0100 0800 0300 1600 0a00  ................
   0x0010:  696d 6473 2d75 6e61 7574 686f 7269 7a65  imds-unauthorize
   0x0020:  6400 0000 0800 0500 0000 0002 0800 0b00  d...............
   0x0030:  0000 0000 0800 0e00 0000 0000 5800 0900  ............X...
   0x0040:  4500 0054 aa6f 4000 4001 3b8f c0a8 4005  E..T.o@.@.;...@.
   0x0050:  a9fe a9fe 0800 20d1 a35d 0001 dabc 7e63  ........]....~c
   0x0060:  0000 0000 15dd 0600 0000 0000 1011 1213  ................
   0x0070:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
   0x0080:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
   0x0090:  3435 3637                                4567


nft -a list ruleset | tee nft.conf
table inet firewall { # handle 2
   set imds_authorized { # handle 3
      type uid
      flags interval
      elements = { 1001 }
   }

   chain input { # handle 1
      type filter hook input priority filter; policy drop;
      ct state established accept # handle 5
      meta nfproto { ipv4, ipv6 } tcp dport 22 accept # handle 6
   }

   chain output { # handle 2
      type filter hook output priority filter; policy accept;
      ip daddr 169.254.0.0/16 meta skuid @imds_authorized log prefix "imds-authorized" group 2 counter packets 0 bytes 0 accept # handle 11
      ip daddr 169.254.0.0/16 log prefix "imds-unauthorized" group 3 counter packets 375 bytes 31500 drop # handle 12
   }
}
```