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
   }
}
```

Logging

Supports NFLog/ulogd2 and syslog

```
nft insert rule inet firewall input handle 5 meta pkttype multicast log prefix "multicast" group 1

tcpdump -ni nflog:1 -XX
18:44:23.134327 IP6 fe80::c095:6dff:fe62:c64 > ff02::1: ICMP6, router advertisement, length 88
   0x0000:  0a00 0001 0800 0100 86dd 0100 0e00 0a00  ................
   0x0010:  6d75 6c74 6963 6173 7400 0000 0800 0400  multicast.......
   0x0020:  0000 0002 1000 0800 0006 0000 c295 6d62  ..............mb
   0x0030:  0c64 0000 0600 0f00 0001 0000 0600 1100  .d..............
   0x0040:  000e 0000 1200 1000 3333 0000 0001 c295  ........33......
   0x0050:  6d62 0c64 86dd 0000 8400 0900 6006 0600  mb.d........`...
   0x0060:  0058 3aff fe80 0000 0000 0000 c095 6dff  .X:...........m.
   0x0070:  fe62 0c64 ff02 0000 0000 0000 0000 0000  .b.d............
   0x0080:  0000 0001 8600 9474 4000 0000 0000 0000  .......t@.......
   0x0090:  0000 0000 0101 c295 6d62 0c64 0501 0000  ........mb.d....
   0x00a0:  0000 05dc 0304 40c0 0027 8d00 0009 3a80  ......@..'....:.
   0x00b0:  0000 0000 fdbf ed26 fb43 e24e 0000 0000  .......&.C.N....
   0x00c0:  0000 0000 1903 0000 0000 010e fe80 0000  ................
   0x00d0:  0000 0000 c095 6dff fe62 0c64             ......m..b.d

nft insert rule inet firewall input handle 5 meta pkttype broadcast log prefix "broadcast " log group 1

journalctl -f
Nov 23 18:49:16 debian kernel: broadcast IN=enp0s1 OUT= MAC=ff:ff:ff:ff:ff:ff:c2:95:6d:62:0c:64:08:00 SRC=192.168.64.1 DST=192.168.64.255
LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=62419 PROTO=ICMP TYPE=8 CODE=0 ID=47846 SEQ=0
```