Default Cumulus Linux ACL Configuration

The Cumulus Linux default ACL configuration is split into three parts, as outlined in the netfilter ACL documentation: IP tables, IPv6 tables, and EB tables. The sections below describe the default configurations for each part. You can see the default file by clicking the Default ACL Configuration link:

Default ACL Configuration

```
cumulus@switch:~$ sudo cl-acltool -L all
--------------------------------
Listing rules of type iptables:
--------------------------------
TABLE filter :
Chain INPUT (policy ACCEPT 167 packets, 16481 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 DROP       all  --  swp+   any     240.0.0.0/5
anywhere
    0     0 DROP       all  --  swp+   any     loopback/8
anywhere
    0     0 DROP       all  --  swp+   any     base-address.mcast.net/8
anywhere
    0     0 DROP       all  --  swp+   any     255.255.255.255
anywhere
    0     0 SETCLASS   udp  --  swp+   any     anywhere
anywhere             udp dpt:3785 SETCLASS  class:7
    0     0 POLICE     udp  --  any    any     anywhere
anywhere             udp dpt:3785 POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   udp  --  swp+   any     anywhere
anywhere             udp dpt:3784 SETCLASS  class:7
    0     0 POLICE     udp  --  any    any     anywhere
anywhere             udp dpt:3784 POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   udp  --  swp+   any     anywhere
anywhere             udp dpt:4784 SETCLASS  class:7
    0     0 POLICE     udp  --  any    any     anywhere
anywhere             udp dpt:4784 POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   ospf --  swp+   any     anywhere
anywhere             SETCLASS  class:7
    0     0 POLICE     ospf --  any    any     anywhere
anywhere             POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   tcp  --  swp+   any     anywhere
anywhere             tcp dpt:bgp SETCLASS  class:7
    0     0 POLICE     tcp  --  any    any     anywhere
anywhere             tcp dpt:bgp POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   tcp  --  swp+   any     anywhere
anywhere             tcp spt:bgp SETCLASS  class:7
    0     0 POLICE     tcp  --  any    any     anywhere
anywhere             tcp spt:bgp POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   tcp  --  swp+   any     anywhere
anywhere             tcp dpt:5342 SETCLASS  class:7
    0     0 POLICE     tcp  --  any    any     anywhere
anywhere             tcp dpt:5342 POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   tcp  --  swp+   any     anywhere
anywhere             tcp spt:5342 SETCLASS  class:7
    0     0 POLICE     tcp  --  any    any     anywhere
```

```
anywhere             tcp spt:5342 POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   icmp --  swp+   any     anywhere
anywhere             SETCLASS  class:2
    1    84 POLICE     icmp --  any    any     anywhere
anywhere             POLICE  mode:pkt rate:100 burst:40
    0     0 SETCLASS   udp  --  swp+   any     anywhere
anywhere             udp dpts:bootps:bootpc SETCLASS  class:2
    0     0 POLICE     udp  --  any    any     anywhere
anywhere             udp dpt:bootps POLICE  mode:pkt rate:100 burst:100
    0     0 POLICE     udp  --  any    any     anywhere
anywhere             udp dpt:bootpc POLICE  mode:pkt rate:100 burst:100
    0     0 SETCLASS   tcp  --  swp+   any     anywhere
anywhere             tcp dpts:bootps:bootpc SETCLASS  class:2
    0     0 POLICE     tcp  --  any    any     anywhere
anywhere             tcp dpt:bootps POLICE  mode:pkt rate:100 burst:100
    0     0 POLICE     tcp  --  any    any     anywhere
anywhere             tcp dpt:bootpc POLICE  mode:pkt rate:100 burst:100
    0     0 SETCLASS   udp  --  swp+   any     anywhere
anywhere             udp dpt:10001 SETCLASS  class:3
    0     0 POLICE     udp  --  any    any     anywhere
anywhere             udp dpt:10001 POLICE  mode:pkt rate:2000 burst:2000
    0     0 SETCLASS   igmp --  swp+   any     anywhere
anywhere             SETCLASS  class:6
    1    32 POLICE     igmp --  any    any     anywhere
anywhere             POLICE  mode:pkt rate:300 burst:100
    0     0 POLICE     all  --  swp+   any     anywhere
anywhere             ADDRTYPE match dst-type LOCAL POLICE  mode:pkt
rate:1000 burst:1000 class:0
    0     0 POLICE     all  --  swp+   any     anywhere
anywhere             ADDRTYPE match dst-type IPROUTER POLICE  mode:pkt
rate:400 burst:100 class:0
    0     0 SETCLASS   all  --  swp+   any     anywhere
anywhere             SETCLASS  class:0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 DROP       all  --  swp+   any     240.0.0.0/5
anywhere
    0     0 DROP       all  --  swp+   any     loopback/8
anywhere
    0     0 DROP       all  --  swp+   any     base-address.mcast.net/8
anywhere
    0     0 DROP       all  --  swp+   any     255.255.255.255
anywhere

Chain OUTPUT (policy ACCEPT 107 packets, 12590 bytes)
 pkts bytes target     prot opt in     out     source
destination


TABLE mangle :
Chain PREROUTING (policy ACCEPT 172 packets, 17871 bytes)
```

```
 pkts bytes target     prot opt in     out     source
destination

Chain INPUT (policy ACCEPT 172 packets, 17871 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 111 packets, 18134 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain POSTROUTING (policy ACCEPT 111 packets, 18134 bytes)
 pkts bytes target     prot opt in     out     source
destination


TABLE raw :
Chain PREROUTING (policy ACCEPT 173 packets, 17923 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 112 packets, 18978 bytes)
 pkts bytes target     prot opt in     out     source
destination


--------------------------------
Listing rules of type ip6tables:
--------------------------------
TABLE filter :
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 DROP       all      swp+   any     ip6-mcastprefix/8
anywhere
    0     0 DROP       all      swp+   any     ::/128
anywhere
    0     0 DROP       all      swp+   any     ::ffff:0.0.0.0/96
anywhere
    0     0 DROP       all      swp+   any     localhost/128
anywhere
    0     0 POLICE     udp      swp+   any     anywhere
anywhere             udp dpt:3785 POLICE  mode:pkt rate:2000 burst:2000
class:7
    0     0 POLICE     udp      swp+   any     anywhere
anywhere             udp dpt:3784 POLICE  mode:pkt rate:2000 burst:2000
class:7
    0     0 POLICE     udp      swp+   any     anywhere
anywhere             udp dpt:4784 POLICE  mode:pkt rate:2000 burst:2000
```

```
class:7
    0     0 POLICE     ospf     swp+   any     anywhere
anywhere             POLICE  mode:pkt rate:2000 burst:2000 class:7
    0     0 POLICE     tcp      swp+   any     anywhere
anywhere             tcp dpt:bgp POLICE  mode:pkt rate:2000 burst:2000
class:7
    0     0 POLICE     tcp      swp+   any     anywhere
anywhere             tcp spt:bgp POLICE  mode:pkt rate:2000 burst:2000
class:7
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmp router-solicitation POLICE  mode:pkt
rate:100 burst:100 class:2
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmp router-advertisement POLICE  mode:pkt
rate:500 burst:500 class:2
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmp neighbour-solicitation POLICE  mode:pkt
rate:400 burst:400 class:2
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmp neighbour-advertisement POLICE  mode:pkt
rate:400 burst:400 class:2
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmptype 130 POLICE  mode:pkt rate:200
burst:100 class:6
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmptype 131 POLICE  mode:pkt rate:200
burst:100 class:6
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmptype 132 POLICE  mode:pkt rate:200
burst:100 class:6
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             ipv6-icmptype 143 POLICE  mode:pkt rate:200
burst:100 class:6
    0     0 POLICE     ipv6-icmp    swp+   any     anywhere
anywhere             POLICE  mode:pkt rate:64 burst:40 class:2
    0     0 POLICE     udp      swp+   any     anywhere
anywhere             udp dpts:dhcpv6-client:dhcpv6-server POLICE
mode:pkt rate:100 burst:100 class:2
    0     0 POLICE     tcp      swp+   any     anywhere
anywhere             tcp dpts:dhcpv6-client:dhcpv6-server POLICE
mode:pkt rate:100 burst:100 class:2
    0     0 POLICE     all      swp+   any     anywhere
anywhere             ADDRTYPE match dst-type LOCAL POLICE  mode:pkt
rate:1000 burst:1000 class:0
    0     0 POLICE     all      swp+   any     anywhere
anywhere             ADDRTYPE match dst-type IPROUTER POLICE  mode:pkt
rate:400 burst:100 class:0
    0     0 SETCLASS   all      swp+   any     anywhere
anywhere             SETCLASS  class:0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
```

```
    0     0 DROP       all      swp+   any     ip6-mcastprefix/8
anywhere
    0     0 DROP       all      swp+   any     ::/128
anywhere
    0     0 DROP       all      swp+   any     ::ffff:0.0.0.0/96
anywhere
    0     0 DROP       all      swp+   any     localhost/128
anywhere

Chain OUTPUT (policy ACCEPT 5 packets, 408 bytes)
 pkts bytes target     prot opt in     out     source
destination


TABLE mangle :
Chain PREROUTING (policy ACCEPT 7 packets, 718 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination


TABLE raw :
Chain PREROUTING (policy ACCEPT 7 packets, 718 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination


--------------------------------
Listing rules of type ebtables:
--------------------------------
TABLE filter :
Bridge table: filter

Bridge chain: INPUT, entries: 16, policy: ACCEPT
```

```
-d BGA -i swp+ -j setclass --class 7 , pcnt = 0 -- bcnt = 0
-d BGA -j police --set-mode pkt --set-rate 2000 --set-burst 2000 , pcnt
= 0 -- bcnt = 0
-d 1:80:c2:0:0:2 -i swp+ -j setclass --class 7 , pcnt = 0 -- bcnt = 0
-d 1:80:c2:0:0:2 -j police --set-mode pkt --set-rate 2000 --set-burst
2000 , pcnt = 0 -- bcnt = 0
-d 1:80:c2:0:0:e -i swp+ -j setclass --class 6 , pcnt = 0 -- bcnt = 0
-d 1:80:c2:0:0:e -j police --set-mode pkt --set-rate 200 --set-burst 200
, pcnt = 0 -- bcnt = 0
-d 1:0:c:cc:cc:cc -i swp+ -j setclass --class 6 , pcnt = 0 -- bcnt = 0
-d 1:0:c:cc:cc:cc -j police --set-mode pkt --set-rate 200 --set-burst
200 , pcnt = 0 -- bcnt = 0
-p ARP -i swp+ -j setclass --class 2 , pcnt = 0 -- bcnt = 0
-p ARP -j police --set-mode pkt --set-rate 400 --set-burst 100 , pcnt =
0 -- bcnt = 0
-d 1:0:c:cc:cc:cd -i swp+ -j setclass --class 7 , pcnt = 0 -- bcnt = 0
-d 1:0:c:cc:cc:cd -j police --set-mode pkt --set-rate 2000 --set-burst
2000 , pcnt = 0 -- bcnt = 0
-p IPv4 -i swp+ -j ACCEPT , pcnt = 0 -- bcnt = 0
-p IPv6 -i swp+ -j ACCEPT , pcnt = 0 -- bcnt = 0
-i swp+ -j setclass --class 0 , pcnt = 0 -- bcnt = 0
-j police --set-mode pkt --set-rate 100 --set-burst 100 , pcnt = 0 --
bcnt = 0
```

```
Bridge chain: FORWARD, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

IP Tables

Action/Value	Protocol/IP Address
Drop Destination IP: Any	Source IPv4: • 240.0.0.0/5 • loopback/8 • 224.0.0.0/4 • 255.255.255.255
Set class: 7 Police: Packet rate 2000 burst 2000 Source IP: Any Destination IP: Any	Protocol: • UDP/BFD Echo • UDP/BFD Control • UDP BFD Multihop Control • OSPF • TCP/BGP (spt dpt 179) • TCP/MLAG (spt dpt 5342)
Set Class: 6 Police: Rate 300 burst 100 Source IP: Any Destination IP: Any	Protocol: • IGMP
Set class: 2 Police: Rate 100 burst 40 Source IP : Any Destination IP: Any	Protocol: • ICMP
Set class: 2 Police: Rate 100 burst 100 Source IP: Any Destination IP: Any	Protocol: • UDP/bootpc, bootps
Set class: 3 Police: Rate 2000 burst:2000 Source IP: Any Destination IP: Any	Protocol: • UDP/LNV

Set class: 0 Police: Rate 1000 burst 1000 Source IP: Any Destination IP: Any	ADDRTYPE match dst-type LOCAL LOCAL is any local address -> Receiving a packet with a destination matching a local IP address on the switch will go to the CPU.
Set class: 0 Police: Rate 400 burst 100 Source IP: Any Destination IP: Any	ADDRTYPE match dst-type IPROUTER IPROUTER is any unresolved address -> On a l2/l3 boundary receiving a packet from L3 and needs to go to CPU in order to ARP for the destination.
Set class 0	All

Set class is internal to the switch - it does not set any precedence bits.

IPv6 Tables

Action/Value	Protocol/IP Address
Drop	Source IPv6: • ff00::/8 • :: • ::ffff:0.0.0.0/96 • localhost
Set class: 7 Police: Packet rate 2000 burst 2000 Source IPv6: Any Destination IPv6: Any	Protocol: • UDP/BFD Echo • UDP/BFD Control • UDP BFD Multihop Control • OSPF • TCP/BGP (spt dpt 179)
Set class: 6 Police: Packet Rte: 200 burst 100 Source IPv6: Any Destination IPv6: Any	Protocol: • Multicast Listener Query (MLD) • Multicast Listener Report (MLD) • Multicast Listener Done (MLD) • Multicast Listener Report V2
Set class: 2 Police: Packet rate: 100 burst 100 Source IPv6: Any Destination IPv6: Any	Protocol: • ipv6-icmp router-solicitation
Set class: 2 Police: Packet rate: 500 burst 500 Source IPv6: Any Destination IPv6: Any	Protocol: • ipv6-icmp router-advertisement POLICE

Set class: 2 Police: Packet rate: 400 burst 400 Source IPv6: Any Destination IPv6: Any	Protocol: • ipv6-icmp neighbour-solicitation • ipv6-icmp neighbour-advertisement
Set class: 2 Police: Packet rate: 64 burst: 40 Source IPv6: Any Destination IPv6: Any	Protocol: • Ipv6 icmp
Set class: 2 Police: Packet rate: 100 burst: 100 Source IPv6: Any Destination IPv6: Any	Protocol: UDP/dhcpv6-client:dhcpv6-server (Spts & dpts)
Police: Packet rate: 1000 burst 1000 Source IPv6: Any Destination IPv6: Any	ADDRTYPE match dst-type LOCAL LOCAL is any local address -> Receiving a packet with a destination matching a local IPv6 address on the switch will go to the CPU.
Set class: 0 Police: Packet rate: 400 burst 100	ADDRTYPE match dst-type IPROUTER IPROUTER is an unresolved address -> On a l2/l3 boundary receiving a packet from L3 and needs to go to CPU in order to ARP for the destination.
Set class 0	All

Set class is internal to the switch - it does not set any precedence bits.

EB Tables

Action/Value	Protocol/MAC Address
Set Class: 7 Police: packet rate: 2000 burst rate:2000 Any switchport input interface	BDPU LACP Cisco PVST
Set Class: 6 Police: packet rate: 200 burst rate: 200 Any switchport input inteface	LLDP CDP
Set Class: 2 Police: packet rate: 400 burst rate: 100 Any switchport input interface	ARP

Catch All: Allow all traffic Any switchport input interface	IPv4 IPv6
Catch All (applied at end): Set class: 0 Police: packet rate 100 burst rate 100 Any switchport	ALL OTHER

> Set class is internal to the switch. It does not set any precedence bits.