Configuring Traffic Analytics

This chapter describes how to configure the Traffic Analytics feature on Cisco NX-OS devices.

About Traffic Analytics

The Traffic Analytics (TA) feature has the following capabilities:

- Provides an ability to identify services offered by servers behind a switch, delivering aggregated analytics data. To distinguish between servers and clients, TCP flags (SYN and SYN ACK) in a three-way handshake are utilized.
- Collapses multiple TCP session data traffic from a client to a server or from a server to client into a single record in the show flow cache database and exports it to the collector. During the traffic analytics aggregation, the source port of TCP is set to a value of 0.

A flow is defined by the source interface, protocol, source IP address, source port, destination IP address, and destination port values. If traffic analytics is enabled, the flows of TCP sessions are aggregated based on source IP address (SIP), destination IP address (DIP), source port (SP) for server to client traffic and SIP, DIP, destination port (DP) for client to server traffic.

Aging of Traffic Database Entries

The traffic database entries will be monitored every 24 hours using a timer. If there is no traffic hitting a database entry, then within 24 to 48 hours that traffic database entry will be deleted. By default the size of the database is 5000.

Troubleshooting Rules

The Troubleshooting rules are used to debug a flow by programming an analytics ACL filter. These rules take precedence over the traffic analytics rules and can be used for capturing specific flow. Troubleshooting rules might result in two entries in the flow cache.

Troubleshooting rules should be used only for specific flows preferably host for short duration only.

Guidelines and Limitations Traffic Analytics

The following guidelines and limitations are applicable to Traffic Analytics:

- Beginning with Cisco NX-OS Release 10.4(2)F, the Traffic Analytics feature is supported on Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 platform switches.
- If the Traffic Analytics feature is enabled, other than TCP all other IP protocols get 3 tuple information.
- The Traffic Analytics feature is supported only on Mixed mode in standalone devices.
- Before enabling the Traffic Analytics feature, ensure to remove the flow filters else an error message will be displayed.
- When a system flow filter is configured, the traffic flow behavior is as follows:
  - If a traffic analytics database has information, two flows are seen in the cache.
  - If a traffic analytics database does not have information, only one flow is seen in the cache.
- If the traffic analytics database size is reduced, new entries will happen only after removing the old entries.
- When NetFlow and traffic analytics are enabled, profiles 29–31 will be used for both functions if we have a scaled NetFlow configuration that is using those profiles. When neighbor discovery or special packets hit these profiles, it is not possible to differentiate whether the record created is traffic analytics or NetFlow. As a result, it gets processed twice, leading to the appearance of two packets with an AN profile.
- Netflow and Flow Telemetry are not supported in N9K-C9364C-H1 platform SFP+ ports, Ethernet1/65, and Ethernet1/66.

Configuring Traffic Analytics

You can configure traffic analytics feature only on mixed mode.

Before you begin

Ensure that you are in mixed mode before enabling the traffic analytics feature. To enable the mixed mode, use the following commands. For more information on mixed mode, see Configuring Mixed Mode:

```
(Config)#feature netflow
(Config)#feature analytics
```

Configure traffic analytics feature as follows:

```
feature analytics
ip access-list telemetryIpv4Acl
permit ip 10.10.10.10/32 20.20.20.20/32
ipv6 access-list telemetryIpv6Acl
permit ipv6 2001:1000::1000:1000/128 2002:1000::1000:1000/128
analytics
  flow filter telemetryFP
  ipv4 telemetryIpv4Acl
  ipv6 telemetryIpv6Acl
flow exporter e11
  destination 10.10.20.21 v9
  transport udp 1100
  events transport udp 55
  source Ethernet1/42
flow exporter e12
  destination 10.10.20.21 v9
  transport udp 9200
  events transport udp 555
  source Ethernet1/42
flow record fte-record
  match ip source address
  match ip destination address
  match ip protocol
  match transport source-port
  match transport destination-port
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
flow monitor m1
  record fte-record
  exporter-bucket-id 1 0 4095
    exporter e11
flow monitor m2
  record fte-record
  exporter-bucket-id 1 0 2000
    exporter e11
  exporter-bucket-id 2 2001 4095
    exporter e12
flow profile telemetryProf
  collect interval 1000
  source port 1001
flow event fte-event1
  group drop-events
    capture buffer-drops
    capture acl-drops
    capture fwd-drops
  group packet-events
    capture tos 50
    capture ttl 50
flow traffic-analytics <<configures the database size>>
    db-size 4500
flow system config
  traffic-analytics <<enables the traffic analytics feature>>
  exporter-id 4
  monitor m1 input
  profile telemetryProf
  event fte-event1
  filter telemetryFP <<enables the Troubleshooting rules>>
```