Configuring Encrypted Traffic Analytics

Restrictions for Encrypted Traffic Analytics

- For SD-Access deployment, ETA is supported on access ports and Wireless VLAN.
- ETA is not supported on management, port-channel, SVI, and loopback interfaces.
- ETA and Cisco Application Visibility and Control (AVC) features can not be applied on the same interface.
- An interface being used as a Flexible NetFlow monitor with ETA enabled, cannot be used to monitor Flexible NetFlow alone on a second target. In such a scenario a separate Flexible NetFlow monitor should be created to monitor the second target.
- ETA and transmit (Tx) Switched Port Analyzer (SPAN) is not supported on the same interface.

Information about Encrypted Traffic Analytics

The following sections provide information about Encrypted Traffic Analytics.

Overview

Encrypted Traffic Analytics (ETA) uses machine learning on an application to determine the flow characteristics such as malware analysis and crypto audit.

Based on the flow-record associated with flow-monitor, the switch creates an exporter template that shows NetFlow records with derived collect fields.

ETA supports multiple templates for the configuration export. There is one template per ETA attribute and ETA sends individual attribute detail in each template during the export. Sequence of Packet Length and

Times (SPLT) and Initial Data Packet (IDP) are stored in separate templates, which are used to generate NetFlow records. Both these NetFlow records are sent for a given application flow.

These templates are sent whenever the data is ready. This helps NetFlow collector to interpret data with correct attribute values. The exporter destination and port is going to be common for all interfaces and this value is provided in the global et-analytics configuration command. The scale number for ETA is 2000 flows per second.

This template export supports only one exporter IP address for an ETA flow-monitor. Multiple template export is supported for NetrFlow v9 version. fromCisco IOS XE Everest 16.6.1

Configuring Flexible NetFlow along with ETA

Flexible NetFlow monitor can be applied on the same interface that has ETA enabled, only if the other flow monitor has the same 5-tuple in the match field. So, Flexible NetFlow with only limited set of match attributes is supported. When Flexible NetFlow monitor and ETA enabled flow monitors are applied on the same physical interface, software merges logically, multiplexing the collect fields and exporter details.

Note While applying two flow monitors on the same interface, if Flexible NetFlow configuration has 5-tuple match, then the Flexible NetFlow monitor should be configured first, and then the et-analytics command should be configured.

If Flexible NetFlow configuration has a different set of match fields, then you will see an error as flow monitor should have only 5-tuple match fields.

When disabling the features et-analytics should be disabled first followed by the Flexible Netflow monitor.

Inactive timer and export

The ETA information is exported only if any of the following two conditions are met.

- If the data required is computed and the required number of packets are seen by the ETA collector.
- If the established flow remains idle for a period configured as inactive timeout, the partial data will be exported.

Note The configured inactive timer is applicable globally. Different ports cannot be configured with different values.

How to Configure Encrypted Traffic Analytics

The following sections provide information on how to configure Encrypted Traffic Analytics.

Configuring Exporter IP and Port

Follow these steps to configure IP address and port.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# config terminal`	Enters the global configuration mode.
Step 3	**et-analytics** **Example:** `Device(config)# et-analytics`	Enters the global et-analytics configuration mode.
Step 4	**ip flow-export destination** *destination_ip_address port* **Example:** `Device(config-et-analytics)# ip flow-export destination 10.1.1.1 2055`	Configures the global collector destination IP address and port.

Configuring Inactive timer value

Follow these steps to configure inactive timer value.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# config t`	Enters the global configuration mode.
Step 3	**et-analytics** **Example:** `Device(config)# et-analytics`	Enters the global et-analytics configuration mode.
Step 4	**inactive time** *time in seconds* **Example:** `Device(config-et-analytics)# inactive time 10`	Configures the inactive timer value. The range is from 1 to 604800 and the default value is 15 seconds.

Enabling Encrypted Traffic Analytics

Follow these steps to enable threat visibility.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# config t`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface gi1/0/2`	Enters the interface configuration mode.
Step 4	**et-analytics enable** **Example:** `Device(config-if)# et-analytics enable`	Enables et-analytics on a particular interface.

Configuration Examples for Encrypted Traffic Analytics

The following sections provide examples for configuring Encrypted Traffic Analytics.

Example: Configuring exporter IP and port

This example shows how to configure a flow-exporter destination IP address of 10.1.1.1 and port 2055.

```
Device#config terminal
Device (config)#et-analytics
Device (config-et-analytics)#ip flow-export destination 10.1.1.1 2055
```

Example: Configuring Inactive timer

This example shows how to configure an inactive timer of 10 seconds.

```
Device#config terminal
Device (config)#et-analytics
Device (config-et-analytics)#inactive time 10
```

Example: Enabling et-analytics

This example shows how to enable et-analytics on interface GigabitEthernet1/0/2.

```
Device#config terminal
Device (config)#interface gi1/0/2
Device (config-if)#et-analytics enable
```

Example: Verifying et-analytics configuration

This example shows how to display global et-analytics configuration.

```
Device#show platform software et-analytics global
ET-Analytics Global state
=========================
All Interfaces : Off
IP Flow-record Destination: 172.26.202.123 : 2055
Inactive timer: 10

ET-Analytics interfaces
GigabitEthernet1/0/26
GigabitEthernet1/0/36

ET-Analytics VLANs
```

This example shows how to display interface et-analytics configuration.

```
Device#show platform software et-analytics interface
ET-Analytics interfaces
GigabitEthernet1/0/3
```

This example shows how to display ETA monitor cache output.

```
Device#show flow monitor etta-mon cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 4

Flows added: 6
Flows aged: 2
- Inactive timeout ( 15 secs) 2

IPV4 DESTINATION ADDRESS: 15.15.15.35
IPV4 SOURCE ADDRESS: 72.163.128.140
IP PROTOCOL: 17
TRNS SOURCE PORT: 53
TRNS DESTINATION PORT: 12032
counter bytes long: 128
counter packets long: 1
timestamp abs first: 06:23:24.799
timestamp abs last: 06:23:24.799
interface input: Null
interface output: Null
```

Additional References

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	Command Reference, Cisco IOS XE Everest 16.6.x (Catalyst 9300 Switches)

Related Topic	Document Title
Flexible NetFlow	Network Management Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 9300 Switches)

Feature History and Information for Encrypted Traffic Analytics

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This feature was introduced.