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 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. If ETA is configured, you do not require to configure NetFlow as NetFlow data for the corresponding flow is also exported along with ETA data.

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 common for all interfaces and this value is provided in the **et-analytics** global 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 NetFlow v9 version.

Encrypted Traffic Analytics 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 the global collector destination 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:**	Configures the global collector destination IP address and port.

	Command or Action	Purpose
	`Device(config-et-analytics)# ip flow-export destination 10.1.1.1 2055`	

Configuring Active-Timeout Value

Follow these steps to configure the active-timeout 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	**active-timeout** *time in seconds* **Example:** `Device(config-et-analytics)# active-timeout 300`	Configures the active-timeout value. The range is from 1 to 604800 and the default value is 30 minutes.

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:**	Enters the global et-analytics configuration mode.

	Command or Action	Purpose
	`Device(config)# et-analytics`	
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 Active-Timeout value

This example shows how to configure the active-timeout value of 300 seconds.

```
Device#config terminal
Device (config)#et-analytics
Device (config-et-analytics)#active-timeout 300
```

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

Feature History for Encrypted Traffic Analytics

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	Encrypted Traffic Analytics	Encrypted Traffic Analytics (ETA) uses machine learning on an application to determine the flow characteristics such as malware analysis and crypto audit.
Cisco IOS XE Amsterdam 17.3.1	Interoperability of Application Visibility and Control and Encrypted Traffic Analytics	Support for interoperability of Application Visibility and Control and Encrypted Traffic Analytics on the same port was introduced.
Cisco IOS XE Bengaluru 17.6.1	Support to configure active-timeout value	Support to configure active-timeout value was introduced. Prior to Cisco IOS XE Bengaluru 17.6.1, the active-timeout value was set to 1800 seconds, by default.
Cisco IOS XE Cupertino 17.7.1	Encrypted Traffic Analytics	This feature was implemented on supervisor modules C9400X-SUP-2 and C9400X-SUP-2XL, which were introduced in this release.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.