Encrypted Traffic Analytics

Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics uses Cisco NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time).

Feature 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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Encrypted Traffic Analytics (ET-Analytics)

Feature Name	Releases	Feature Information
Encrypted Traffic Analytics	Cisco IOS XE Everest 16.6.2	Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics uses Cisco NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time).

Restrictions for Encrypted Traffic Analytics

ET-Analytics is not supported on management interfaces, VRF-Aware Software Infrastructure (VASI) interface, and internal interfaces.

Information About Encrypted Traffic Analytics

Data Elements for Encrypted Traffic

ET-Analytics uses intraflow metadata to identify malware components, maintaining the integrity of the encrypted traffic without the need for bulk decryption and without compromising on data integrity.

ET-Analytics extracts the following main data elements from the network flow: the sequence of packet lengths and times (SPLT), TLS-specific features, and the initial data packet (IDP). Cisco's Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network. Separate templates can be defined for each of the data elements.

Transport Layer Security (TLS) is a cryptographic protocol that provides privacy for applications. TLS is usually implemented with common protocols such as HTTP for web browsing or Simple Mail Transfer Protocol (SMTP) for email. HTTPS is the use of TLS over HTTP; this protocol is used to secure communication between a web server and client and is supported by most major web servers.

The TLS template is used to report several of the TLS parameters in use for a flow. These parameters help in finding the use of insecure cipher suites, out-of-date protocol version, and so on.

- Sequence of Packet Lengths and Times (SPLT) SPLT contains the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the inter-arrival times of those packets. SPLT can be represented as an array of packet sizes (in bytes) along with an array of times (in milliseconds) indicating the time since the previous packet was observed. The SPLT template is used to report packet size and timing information for a flow, which is useful to analyze encrypted traffic and find malicious flows or perform other classifications.
- Initial Data Packet (IDP) IDP obtains packet data from the first packet of a flow. It allows extraction of data such as an HTTP URL, DNS hostname/address, and other data elements. The TLS handshake is composed of several messages that contain unencrypted metadata used to extract data elements such as cipher suites, TLS versions, and the client's public key length. The IDP template is used to report packet data from the first data packet of a flow. This template allows collectors to perform application classification of a flow (for example, using Snort).

How to Configure Encrypted Traffic Analytics

Enabling ET-Analytics on an Interface

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**et-analytics**	Enters encrypted traffic analytics configuration mode.
Step 4	**ip flow-record destination** *ip-address port*	Specifies NetFlow collector IP address and port number. A maximum of four exporters is supported.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**interface** *interface-id*	Specifies the interface and port number and enters interface configuration mode.
Step 7	**et-analytics enable**	Enables encrypted traffic analytics on this interface.
Step 8	**end**	Returns to privileged EXEC mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-record destination 192.0.2.1 2055
Device(config-et-analytics)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# et-analytics enable
Device(config-if)# end
```

Applying an ACL for Whitelisting

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
		• Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**et-analytics**	Enters encrypted traffic analytics configuration mode.
Step 4	**whitelist acl** *access-list*	Whitelists the specified access list traffic. The access list can be a standard, extended, or named ACL.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**ip access-list extended** *access-list*	Specifies a named extended access list and enters extended access list configuration mode.
Step 7	**permit ip** {*ip-address* | **any** | **host** | **object-group**}	Specifies the packets to forward to a source host or source IP address.
Step 8	**end**	Returns to privileged EXEC mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl eta_whitelist
Device(config-et-analytics)# exit
Device(config)# ip access-list extended eta_whitelist
Device(config-ext-nacl)# permit ip host 198.51.100.1 any
Device(config-ext-nacl)# permit ip any host 198.51.100.1
Device(config-ext-nacl)# permit ip host 198.51.200.1 any
Device(config-ext-nacl)# permit ip any host 198.51.200.1
Device(config-ext-nacl)# end
```

Verifying the ET-Analytics Configuration

The following **show** commands are used to see the platform ET-analytics, threat-visibility interfaces, FMAN FP global and interface information, and ET-analytics datapath information. Given below are the sample outputs of the **show** commands.

```
Device# show platform hardware qfp active feature et-analytics data interface gigabitEthernet
 2

uidb handle: 0x3fe
Interface Name: GigabitEthernet2
```

```
Device# show platform hardware qfp active feature et-analytics data memory

  ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 952903
   No. of FO frees       : 952902


Device# show platform hardware qfp active feature et-analytics data runtime

  ET-Analytics run-time information:

   Feature state         : initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   Flow CFG information  :   !Flow Table Infrastructure information internal to ETA!
       instance ID       : 0x0
       feature ID        : 0x0
       feature object ID : 0x0
       chunk ID          : 0x4


Device# show platform hardware qfp active feature et-analytics datapath stats export

  ET-Analytics 192.168.1.100:2055 Stats:
    Export statistics:
      Total records exported     : 2967386
      Total packets exported     : 1885447
      Total bytes exported       : 2056906120
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 805813
            responder->initiator : 418799
      Total SPLT records exported:
            initiator->responder : 805813
            responder->initiator : 418799
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 171332
            responder->initiator : 174860
ET-Analytics 172.27.56.99:2055 Stats:
    Export statistics:
      Total records exported     : 2967446
      Total packets exported     : 1885448
      Total bytes exported       : 2056909280
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 805813
            responder->initiator : 418799
      Total SPLT records exported:
            initiator->responder : 805813
```

```
          responder->initiator : 418799
   Total SALT records exported:
          initiator->responder : 0
          responder->initiator : 0
      Total BD records exported  :
          initiator->responder : 0
          responder->initiator : 0
      Total TLS records exported :
          initiator->responder : 171332
          responder->initiator : 174860
```

Device# show platform hardware qfp active feature et-analytics datapath stats flow

```
  ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```