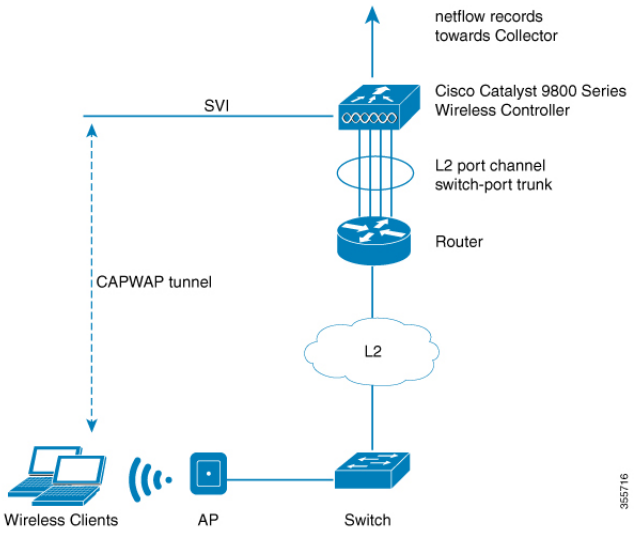
Encrypted Traffic Analytics

Information About Encrypted Traffic Analytics

The Encrypted Traffic Analytics (ETA) leverages Flexible NetFlow (FNF) technology to export useful information about the flow to the collectors and gain visibility into the network.

Figure 1: Encrypted Traffic Analytics Deployed on Cisco Catalyst 9800 Series Wireless Controller in Local Mode



The wireless clients send data packets to the access point. The packets are then CAPWAP encapsulated and sent to the controller. This means that the actual client data is in the CAPWAP payload. To apply ETA on the client data, you need to strip the CAPWAP header before handing over the packet to the ETA module.

The ETA offers the following advantages:

- Enhanced telemetry based threat analytics.
- Analytics to identify malware.

Exporting Records to IPv4 Flow Export Destination

Follow the procedure given below to enable encrypted traffic analytics and configure a flow export destination:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**ip flow-export destination** *ip_address port_number* **Example:** `Device(config-et-analytics)# ip flow-export destination 120.0.0.1 2055`	Configures the NetFlow record export. Here, *port_number* ranges from 1 to 65535.
Step 4	**end** **Example:** `Device(config-et-analytics)# end`	Returns to privileged EXEC mode.

Configuring ETA Flow Export Destination (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **NetFlow**.

Step 2 Click the **Add** button. The **Create NetFlow** dialog box appears.

Step 3 Choose any one of the available templates from the **NetFlow Template** drop-down list.

Step 4 Enter an IPv4 or IPv6 address in the **Collector Address** field.

Step 5 Enter a port number in the **Exporter Port** field. You must specify a value between 1 and 65535.

Step 6 Choose the desired option from the **Export Interface IP** drop-down list.

Step 7 Choose any one of the sampling methods from the **Sampling Method** drop-down list. The available options are **Deterministic**, **Random**, and **Full Netflow**.

Step 8 Enter a range for the sample. You must specify a value between 32 and 1032.

Step 9 Select the required interfaces/profile from the **Available** pane and move it to the **Selected** pane.

Step 10 Click the **Save & Apply to Device** button.

Enabling In-Active Timer

Follow the procedure given below to enable in-active timer:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Configures the encrypted traffic analytics.
Step 3	**inactive-timeout** *timeout-in-seconds* **Example:** `Device(config-et-analytics)# inactive-timeout 15`	Specifies the inactive flow timeout value. Here, *timeout-in-seconds* ranges from 1 to 604800.
Step 4	**end** **Example:** `Device(config-et-analytics)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Enabling ETA on WLAN Policy Profile

Follow the procedure given below to enable ETA on WLAN policy profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**et-analytics enable** **Example:** `Device(config-wireless-policy)# et-analytics enable`	Enables encrypted traffic analytics on the policy.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching Policy Profile to VLAN (GUI)

Perform the following steps to attach a policy profile to VLAN.

Procedure

Step 1 Check the **RADIUS Profiling** checkbox.

Step 2 From the **Local Subscriber Policy Name**, choose the required policy name.

Step 3 In the **WLAN Local Profiling** section, enable or disable the **Global State of Device Classification**, check the checkbox for **HTTP TLV Caching** and **DHCL TLV Caching**.

Step 4 In the **VLAN** section, choose the **VLAN/VLAN Group** from the drop-down list. Enter the Multicast VLAN.

Step 5 In the **WLAN ACL** section, choose the **IPv4 ACL** and **IPv6 ACL** from the drop-down list.

Step 6 In the **URL Filters** section, choose the **Pre Auth** and **Post Auth** from the drop-down list.

Step 7 Click **Save & Apply to Device**.

Attaching Policy Profile to VLAN

Follow the procedure given below to attach a policy profile to VLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan vlan-name`	Assigns the policy profile to the VLANs.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.

Verifying ETA Configuration

Verifying ETA Globally

To view the ETA global and interface details, use the following command:

```
Device# show platform software utd chassis active F0 et-analytics global

ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```

To view the ETA global configuration, use the following command:

```
Device# show platform software et-analytics global

ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 192.168.5.2 : 2055
 Inactive timer: 15
```

Note The **show platform software et-analytics global** command does not display the ETA enabled wireless client interfaces.

To view the ETA global state in datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime

ET-Analytics run-time information:

   Feature state: initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   WhiteList information :
```

```
       flag: False
       cgacl w0 :  n/a
       cgacl w1 :  n/a
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x1
       feature object ID : 0x1
       chunk ID : 0xC
```

To view the ETA memory details, use the following command:

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

ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 0
   No. of FO frees       : 0
```

To view the ETA flow export in datapath, use the following command:

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

ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
    Export statistics:
      Total records exported     : 5179231
      Total packets exported     : 3124873
      Total bytes exported       : 3783900196
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      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 : 309937
            responder->initiator : 329469
```

To view the ETA flow statistics, use the following command:

```
Device# show platform hardware chassis active qfp 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
```

Verifying ETA on Wireless Client Interface

To view if a policy is configured with ETA, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : 160
Multicast VLAN                : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : ENABLED
  Flex NAT PAT            : DISABLED
  Central Assoc               : ENABLED
```

To view the ETA status in the wireless client detail, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
<client_mac>

Wlclient Details for Client mac: 0026.c635.ebf8
  ---------------------------------
    Input VlanId  :  160
    Point of Presence      :  0
    Wlclient Input flags   :  9
    Instance ID   :  3
    ETA enabled   :  True
    client_mac_addr        :  0026.c635.ebf8

    bssid_mac_addr:  58ac.7843.037f
    Point of Attachment    :  65497
    Output vlanId :  160
    wlan_output_uidb       :  -1
    Wlclient Output flags  :  9
    Radio ID :  1
    cgacl w0 :  0x0
    cgacl w1 :  0x0
    IPv6 addr number       :  0
    IPv6 addr learning     :  0
```

To view clients in the ETA pending wireless client tree, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree

CPP IF_H     DPIDX      MAC Address    VLAN  AS  MS WLAN          POA
------------------------------------------------------------------------------
   0X2A     0XA0000001  2c33.7a5b.827b  160   RN  LC xyz_ssid     0x90000003
   0X2B     0XA0000002  2c33.7a5b.80fb  160   RN  LC xyz_ssid     0x90000003
```

To view the QFP interface handle, use the following command:

```
Device#
show platform hardware chassis active qfp interface if-handle <qfp_interface_handle>
```

```
show platform hardware chassis active qfp interface if-handle 0X29
FIA handle - CP:0x27f3ce8  DP:0xd7142000
  LAYER2_IPV4_INPUT_ARL_SANITY
  WLCLIENT_INGRESS_IPV4_FWD
  IPV4_TVI_INPUT_FIA         >>> ETA FIA Enabled
  SWPORT_VLAN_BRIDGING
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x27f3d30  DP:0xd7141780
  IPV4_VFR_REFRAG (M)
  IPV4_TVI_OUTPUT_FIA        >>> ETA FIA Enabled
  WLCLIENT_EGRESS_IPV4_FWD
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

Note The *qfp_interface_handle* ranges from 1 to 4294967295.

To view the ETA pending wireless client tree statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics statistics

Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                          Value
-----------------------------------------------------------------
Enable ETA on wireless client called             0
Delete ETA on wireless client called             0
ETA global cfg init cb TVI FIA enable error      0
ETA global cfg init cb output SB read error      0
ETA global cfg init cb output SB write error     0
ETA global cfg init cb input SB read error       0
ETA global cfg init cb input SB write error      0
ETA global cfg init cb TVI FIA enable success    0
ETA global cfg uninit cb ingress feat disable    0
ETA global cfg uninit cb ingress cfg delete e    0
ETA global cfg uninit cb egress feat disable     0
ETA global cfg uninit cb egress cfg delete er    0
ETA pending list insert entry called             4
ETA pending list insert invalid arg error        0
ETA pending list insert entry exists error       0
ETA pending list insert no memory error          0
ETA pending list insert entry failed             0
ETA pending list insert entry success            4
ETA pending list delete entry called             2
ETA pending list delete invalid arg error        0
ETA pending list delete entry missing            0
ETA pending list delete entry remove error       0
ETA pending list delete entry success            2
```