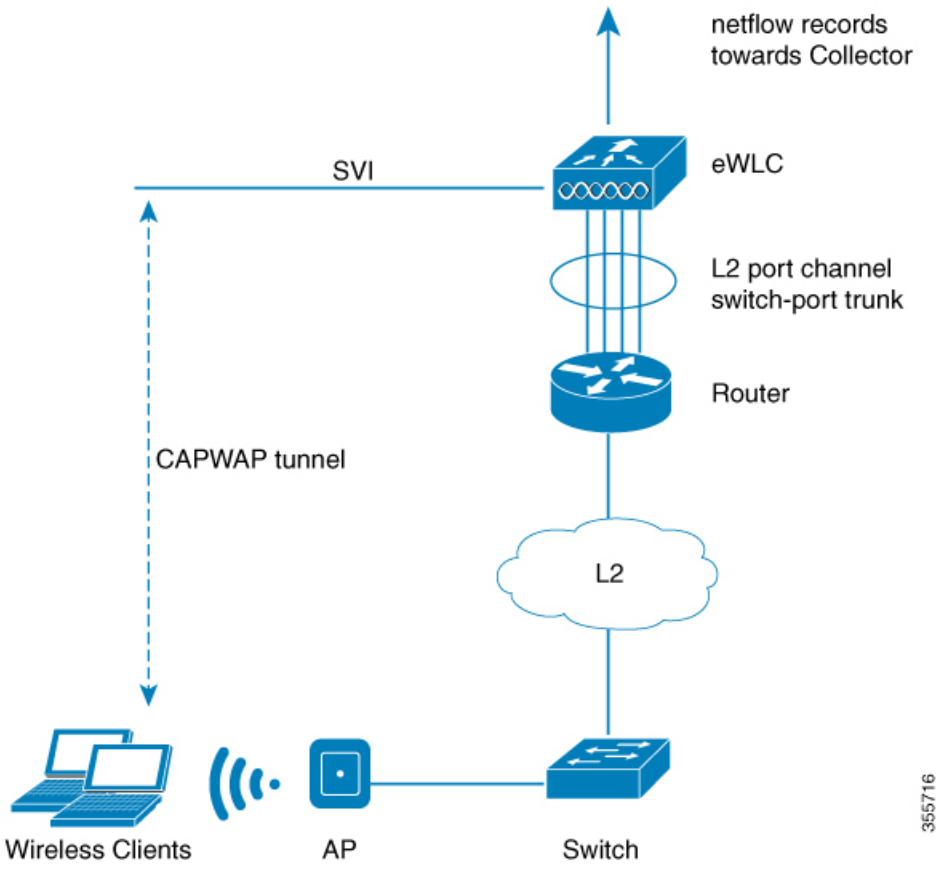
SD-Access（SDA ワイヤレス）での暗号化トラフィック分析の設定

暗号化トラフィック分析について

暗号化トラフィック分析（ETA）は、Flexible Netflow（FNF）テクノロジーを利用してフローに関する有用な情報をコレクタにエクスポートし、ネットワークの可視化を実現します。

図 *1:* ローカル モードの *Cisco Catalyst 9800* シリーズ ワイヤレス コントローラに導入された暗号化トラフィック分析



ワイヤレス クライアントはデータ パケットをアクセス ポイントに送信します。次にパケットは CAPWAP によってカプセル化され、コントローラに送信されます。つまり、実際のクライアント データは CAPWAP ペイロードに含まれています。ETA をクライアント データに適用するには、パケットを ETA モジュールに渡す前に CAPWAP ヘッダーを除去する必要があります。

ETA には、次のような利点があります。

- 強化されたテレメトリ ベースの脅威分析。
- 分析によるマルウェアの特定。

ETA のグローバルな有効化

ETA の有効化

暗号化トラフィック分析を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**et-analytics** 例： `Device(config)# et-analytics`	暗号化トラフィック分析を設定します。
ステップ 3	**end** 例： `Device(config-et-analytics)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ETA フロー エクスポートの宛先の設定

ETA フロー エクスポートの宛先を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**et-analytics** 例： `Device(config)# et-analytics`	暗号化トラフィック分析を設定します。
ステップ 3	**ip flow-export destination** *ip_address port_number* 例： `Device(config-et-analytics)# ip flow-export destination 120.0.0.1 2055`	NetFlow レコードのエクスポートを設定します。 ここで、各変数は次のように定義されます。 *port_number* の範囲は 1 ～ 65535 です。
ステップ 4	**end** 例： `Device(config-et-analytics)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ETA フロー エクスポートの宛先の設定（GUI）

手順

ステップ 1 [Configuration] > [Services] > [NetFlow] を選択します。

ステップ 2 [Add] ボタンをクリックします。[Create NetFlow] ダイアログ ボックスが表示されます。

ステップ 3 [Netflow Template] ドロップダウンリストから、使用可能なテンプレートのいずれかを選択します。

ステップ 4 [Collector Address] フィールドに IP アドレスを入力します。

ステップ 5 [Exporter Port] フィールドにポート番号を入力します。1 ～ 65535 の範囲で値を指定する必要があります。

ステップ 6 [Export Interface IP] ドロップダウンリストから必要なオプションを選択します。

ステップ 7 [Sampling Method] ドロップダウンリストから、いずれかのサンプリング方式を選択します。使用可能なオプションは、[Deterministic]、[Random]、および [Full Netflow] です。

ステップ 8 サンプルの範囲を入力します。32 ～ 1032 の値を指定する必要があります。

ステップ 9 [Available] ペインから必要なインターフェイスを選択して [Selected] ペインに移動します。

ステップ 10 [Save & Apply to Device] ボタンをクリックします。

非アクティブ タイマーの有効化

非アクティブ タイマーを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**et-analytics** 例： `Device(config)# et-analytics`	暗号化トラフィック分析を設定します。
ステップ 3	**inactive-timeout** *timeout-in-seconds* 例： `Device(config-et-analytics)# inactive-timeout 15`	非アクティブ フローのタイムアウト値を指定します。 *timeout-in-seconds* の範囲は 1 ～ 604800 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-et-analytics)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN ポリシー プロファイルでの ETA の有効化

WLAN ポリシー プロファイルで ETA を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**et-analytics enable** 例： `Device(config-wireless-policy)# et-analytics enable`	ポリシーで暗号化トラフィック分析を有効にします。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

VLAN へのポリシー プロファイルの適用（GUI）

VLAN にポリシー プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1 [RADIUS Profilling] チェックボックスをオンにします。

ステップ 2 [Local Subscriber Policy Name] から必要なポリシー名を選択します。

ステップ 3 [WLAN Local Profiling] セクションで [Global State of Device Classification] を有効または無効にして、[HTTP TLV Caching] と [DHCL TLV Caching] のチェックボックスをオンにします。

ステップ 4 [VLAN] セクションで、ドロップダウンリストから [VLAN/VLAN Group] を選択します。マルチキャスト VLAN を入力します。

ステップ 5 [WLAN ACL] セクションで、ドロップダウンリストから [IPv4 ACL] と [IPv6 ACL] を選択します。

ステップ 6 [URL Filters] セクションで、ドロップダウンリストから [Pre Auth] と [Post Auth] を選択します。

ステップ 7 [Save & Apply to Device] をクリックします。

VLAN へのポリシー プロファイルの適用

VLAN にポリシー プロファイルを適用するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile policy** *profile-name* **例：** `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**vlan** *vlan-name* **例：** `Device(config-wireless-policy)# vlan vlan-name`	ポリシー プロファイルを VLAN に割り当てます。
ステップ 4	**no shutdown** **例：** `Device(config-wireless-policy)# no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。

ETA 設定の確認

ETA のグローバルな確認

ETA グローバルおよびインターフェイスの詳細を表示するには、次のコマンドを使用します。

```
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
```

ETA グローバル設定を表示するには、次のコマンドを使用します。

```
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
```

（注） **show platform software et-analytics global** コマンドでは、ETA が有効になっているワイヤレス クライアント インターフェイスは表示されません。

データパスの ETA グローバル状態を表示するには、次のコマンドを使用します。

```
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
```

ETA メモリの詳細を表示するには、次のコマンドを使用します。

```
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
```

データパスの ETA フロー エクスポートを表示するには、次のコマンドを使用します。

```
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
```

ETA フローの統計情報を表示するには、次のコマンドを使用します。

```
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
```

ワイヤレス クライアント インターフェイス上の ETA の確認

ポリシーに ETA が設定されているかどうかを確認するには、次のコマンドを使用します。

```
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
```

ワイヤレス クライアントの詳細で ETA ステータスを表示するには、次のコマンドを使用します。

```
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
```

ETA 保留ワイヤレス クライアント ツリー内のクライアントを表示するには、次のコマンドを使用します。

```
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
```

QFP インターフェイス ハンドルを表示するには、次のコマンドを使用します。

```
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)
```

（注） *qfp_interface_handle* の範囲は 1 ～ 4294967295 です。

ETA 保留ワイヤレス クライアント ツリーの統計情報を表示するには、次のコマンドを使用します。

```
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
```