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の制約事項

- ETA は、アクセス ポートと SDA 導入環境のワイヤレス VLAN でのみサポートされています。管理、トランク、ポートチャネル、SVI、ループバックの各インターフェイスではサポートされていません。
- ETA および Cisco Application Visibility and Control（AVC）の機能は、同じインターフェイスには適用できません。
- ETA が有効になっている Flexible NetFlow モニターとして使用されているインターフェイスは、2 番目のターゲットで Flexible NetFlow のみをモニターするためには使用できません。このようなシナリオでは、別の Flexible NetFlow モニターを作成して 2 番目のターゲットをモニターする必要があります。
- ETA と送信（Tx）スイッチドポートアナライザ（SPAN）は、同じインターフェイスではサポートされません。

暗号化トラフィック分析について

ここでは、暗号化トラフィック分析について説明します。

概要

暗号化トラフィック分析（ETA）はアプリケーションに機械学習を使用して、マルウェア分析や暗号監査などのフロー特性を特定します。

フローモニターに関連付けられた フローレコードに基づき、派生収集フィールドを使用して NetFlow レコードを表示するエクスポータ テンプレートをスイッチが作成します。

ETA は、設定のエクスポート用の複数のテンプレートをサポートします。ETA 属性ごとに 1 つのテンプレートがあり、ETA は各テンプレートの個々の属性の詳細をエクスポート時に送信します。パケット長と時間のシーケンス（SPLT）および初期データ パケット（IDP）は、別個のテンプレートに格納され、NetFlow レコードの生成に使用されます。これらの NetFlow レコードの両方が、指定のアプリケーション フローに送信されます。

これらのテンプレートは、データの準備が整うたびに送信されます。これにより、NetFlow コレクタは正しい属性値でデータを解釈することができます。エクスポータの宛先とポートがすべてのインターフェイスに共通となり、この値がグローバル et-analytics コンフィギュレーション コマンドで提供されます。ETA のスケール数は 2000 フロー/秒です。

このテンプレート エクスポートは、ETA フローモニターで 1 つのエクスポータ IP アドレスのみをサポートします。複数テンプレートのエクスポートは、以降の NetrFlow v9 バージョンでサポートされます

Flexible NetFlow と ETA の設定

Flexible NetFlow モニターは、他のフローモニターの一致フィールドに同じ 5 タプルがある場合にのみ、ETA が有効になっている同じインターフェイスに適用できます。そのため、限定された一連の一致属性のみを持つ Flexible NetFlow がサポートされます。Flexible NetFlow モニタと ETA に対応するフロー モニタを同じ物理インターフェイスに適用すると、ソフトウェアは論理的にマージし、収集フィールドとエクスポータの詳細を多重化します。

（注） 2 つのフローモニターを同じインターフェイスに適用している間、Flexible NetFlow 設定に 5 タプルの一致がある場合は、Flexible NetFlow モニターを最初に設定してから、et-analytics コマンドを設定する必要があります。

Flexible NetFlow 設定に一連の異なる一致フィールドがある場合はエラーが表示されます。これは、フローモニターに必要なのが 5 タプルの一致フィールドのみであるためです。

機能を無効にする場合は、最初に et-analytics を無効にしてから、Flexible Netflow モニターを無効にする必要があります。

非アクティブ タイマーとエクスポート

次の 2 つの条件のいずれかが満たされた場合にのみ ETA 情報がエクスポートされます。

- 必要なデータが計算され、ETA コレクタによって必要な数のパケットが確認された場合。

- 確立されたフローが非アクティブタイムアウトとして設定された期間にわたってアイドル状態のままになっていて、一部のデータがエクスポートされる場合。

（注） 設定した非アクティブタイマーはグローバルに適用されます。異なるポートを異なる値で設定することはできません。

暗号化トラフィック分析の設定方法

ここでは、暗号化トラフィック分析の設定方法について説明します。

エクスポータ IP とポートの設定

IP アドレスとポートを設定するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# config 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 3	**et-analytics** 例： `Device(config)# et-analytics`	グローバル et-analytics コンフィギュレーション モードを開始します。
ステップ 4	**ip flow-export destination** *destination_ip_address port* 例： `Device(config-et-analytics)# ip flow-export destination 10.1.1.1 2055`	グローバル コレクタの宛先 IP アドレスとポートを設定します。

非アクティブ タイマー値の設定

非アクティブ タイマー値を設定するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# config t`	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 3	**et-analytics** 例： `Device(config)# et-analytics`	グローバル et-analytics コンフィギュレーション モードを開始します。
ステップ 4	**inactive time** *time in seconds* 例： `Device(config-et-analytics)# inactive time 10`	非アクティブタイマー値を設定します。範囲は 1 ～ 604800 で、デフォルトは 15 秒です。

暗号化トラフィック分析の有効化

脅威の可視性をイネーブルにするには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# config t`	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 3	**interface** *interface-id* 例： `Device(config)# interface gi1/0/2`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**et-analytics enable** 例： `Device(config-if)# et-analytics enable`	特定のインターフェイス上で et-analytics イネーブルにします。

暗号化トラフィック分析の設定例

ここでは、暗号化トラフィック分析の設定例を示します。

例：エクスポータ IP とポートの設定

次に、フローエクスポータの宛先 IP アドレスを 10.1.1.1 に、ポートを 2055 に設定する例を示します。

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

例：非アクティブ タイマーの設定

次に、非アクティブ タイマーを 10 秒に設定する例を示します。

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

例：et-analytics の有効化

次に、インターフェイス GigabitEthernet1/0/2 で et-analytics を有効にする例を示します。

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

例：et-analytics 設定の確認

次に、グローバル et-analytics コンフィギュレーションを表示する例を示します。

```
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
```

次に、インターフェイス et-analytics コンフィギュレーションを表示する例を示します。

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

次に、ETA モニター キャッシュ出力を表示する例を示します。

```
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
```

その他の参考資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	Cisco IOS XE Everest 16.6.x（Catalyst 9300 スイッチ）コマンド リファレンス
Flexible NetFlow	Cisco IOS XE Everest 16.6.x（Catalyst 9300 スイッチ）ネットワーク管理コンフィギュレーション ガイド

暗号化トラフィック分析の機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。