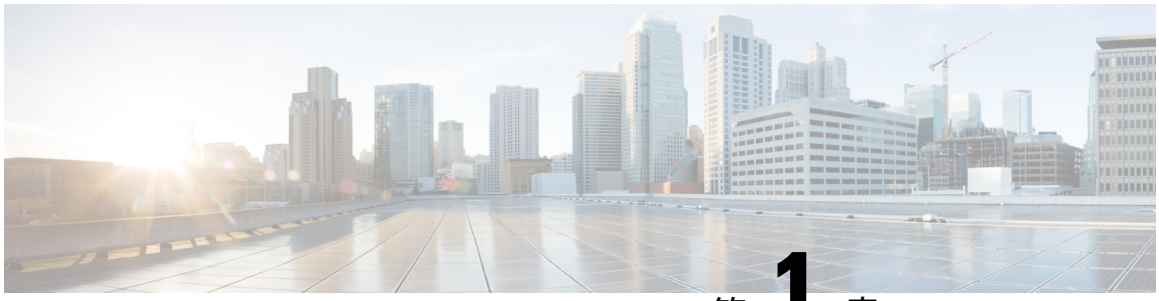
暗号化トラフィック分析コンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

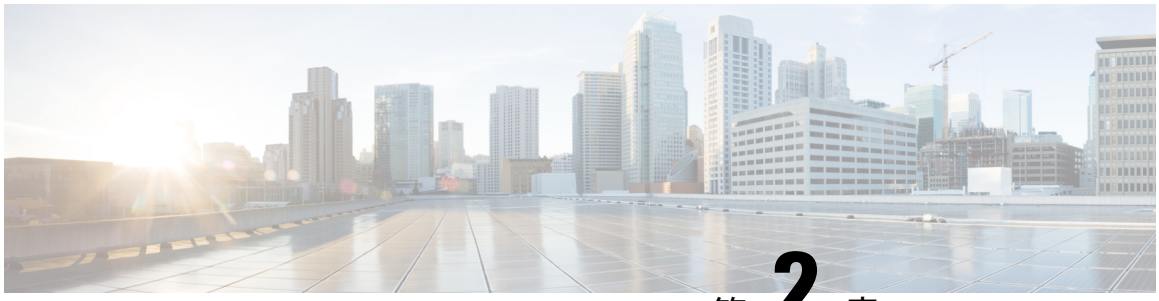
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- Cisco IOS Command References, All Releases

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

暗号化トラフィック分析

暗号化トラフィック分析（ET 分析）は、暗号化トラフィック内に潜むマルウェア通信を特定するために使用されます。ET 分析では、パッシブ モニタリングや関連データ要素の抽出、クラウドベースのグローバルな可視性を備える管理された機械学習を使用します。ET分析では、関連データ要素を NetFlow レコード フィールドの形式でエクスポートして、パケット フローにマルウェアがあるかどうかを検出します。この NetFlow レコード フィールドには、IDP（初期データ パケット）と SPLT（パケット長とパケット時間のシーケンス）が含まれています。

暗号化トラフィック分析の機能について

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 リリースのみを示しています。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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* 暗号化トラフィック分析（*ET* 分析）の機能について

機能名	リリース	機能情報
暗号化トラフィック分析	Cisco IOS XE Fuji 16.7.1 Cisco IOS XE Everest 16.6.2	暗号化トラフィック分析（ET 分析）は、暗号化トラフィック内に潜むマルウェア通信を特定するために使用されます。ET 分析では、パッシブモニタリングや関連データ要素の抽出、クラウドベースのグローバルな可視性を備える管理された機械学習を使用します。ET 分析では、関連データ要素を NetFlow レコード フィールドの形式でエクスポートして、パケットフローにマルウェアがあるかどうかを検出します。この NetFlow レコード フィールドには、IDP（初期データ パケット）と SPLT（パケット長とパケット時間のシーケンス）が含まれています。
暗号化トラフィック分析	Cisco IOS XE Fuji 16.8.1	フロー先での VRF キーワードのサポートが追加されました。

暗号化トラフィック分析の制約事項

ET 分析は、管理インターフェイス、VRF 対応ソフトウェア インフラストラクチャ（VASI）インターフェイス、および内部インターフェイスではサポートされていません。

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のデータ要素

ET 分析では、イントラフロー メタデータを使用してマルウェア コンポーネントを特定します。一括復号を行わなくてもデータの整合性を損なうことなく暗号化トラフィックの整合性を維持できます。

ET 分析では、ネットワーク フローから主要なデータ要素として、パケット長とパケット時間のシーケンス（SPLT）、TLS 固有の特長、および初期データ パケット（IDP）を抽出します。シスコの特定用途集積回路（ASIC）アーキテクチャは、データ ネットワークの速度を低下させずにこれらのデータ要素を抽出することができます。データ要素ごとに個別のテンプレートを定義できます。

Transport Layer Security（TLS）はアプリケーションにプライバシーを提供する暗号化プロトコルです。TLS は通常、Web 閲覧で使用する HTTP や電子メールで使用する Simple Mail Transfer Protocol（SMTP）のような共通プロトコルとともに実装されます。HTTPS は HTTP 通信に TLS を使う方法です。このプロトコルは、Web サーバとクライアントとの間の通信をセキュアにするために使用され、ほとんどの主要な Web サーバでサポートされています。

TLS テンプレートは、フローで使用されている TLS パラメータのいくつかをレポートするために使用されます。これらのパラメータは、安全でない暗号スイートや古いプロトコル バージョンなどの使用を見つけるうえで役立ちます。

- パケット長とパケット時間のシーケンス（SPLT）：SPLT にはパケット間の着信時間の間隔に加えて、各パケットのアプリケーション ペイロードの長さ（バイト数）が含まれます。SPLT は、一連のパケット サイズ（単位：バイト）を、1 つ前のパケットがモニタされてからの一連の時間（単位：ミリ秒）とともに表すことができます。SPLT テンプレートは、フローのパケットサイズとタイミング情報をレポートするために使用されます。これは、暗号化トラフィックを分析して悪意のあるフローを見つけたり、他の分類を実行したりするうえで役立ちます。
- 初期データ パケット（IDP）：IDP は、フローの最初のパケットからパケット データを取得します。IDP により、HTTP URL、DNS ホスト名、IP アドレスなどのデータを抽出できます。TLS ハンドシェイクは、非暗号化メタデータを持つ複数のメッセージで構成されます。メタデータは、暗号スイート、TLS のバージョン、クライアントの公開キー長などデータ要素の抽出に使用します。IDP テンプレートは、フローの最初のデータ パケットから取得したパケットデータをレポートするために使用されます。このテンプレートを使用すると、コレクタはフローのアプリケーション分類を実行できます（たとえば、Snort を使用して実行します）。

暗号化トラフィック分析の設定方法

インターフェイスでの ET 分析の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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**	暗号化トラフィック分析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** *ip-address port* [**vrf** *vrf-name*]	宛先 IP アドレスのオプションの VRF 名を設定します。ETA レコードはこの宛先にエクスポートされます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**interface** *interface-id*	インターフェイスとポート番号を指定して、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 7	**et-analytics enable**	このインターフェイスで暗号化トラフィック分析を有効にします。
ステップ 8	**end**	特権 EXEC モードに戻ります。

例

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

ホワイトリストに登録するための ACL の適用

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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**	暗号化トラフィック分析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	**whitelist acl** *access-list*	指定されたアクセス リスト トラフィックをホワイトリストに登録します。アクセスリストには標準、拡張、または名前付き ACL を使用できます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip access-list extended** *access-list*	名前付き拡張アクセス リストを指定し、拡張アクセス リスト コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**permit ip** {*ip-address* | **any** | **host** | **object-group**}	送信元ホストまたは送信元IPアドレスに転送するパケットを指定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。

例

```
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
```

ET 分析設定の確認

次の **show** コマンドを使用すると、プラットフォーム ET 分析、脅威の可視化インターフェイス、FMAN FP のグローバル情報とインターフェイス情報、および ET 分析のデータパス情報が表示されます。以下に、**show** コマンドの出力例を示します。

```
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 vrf 2 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
```

Device# show vrf tableid

```
VRF Name                            Tableid             Address Family
Mgmt-intf                           0x00000001          ipv4 unicast
Mgmt-intf                           0x1E000001          ipv6 unicast
blu                                 0x00000002          ipv4 unicast
red                                 0x00000003          ipv4 unicast
```