



Cisco Secure Cloud Analytics

拡張 NetFlow 設定ガイド



目次

拡張 NetFlow 向け設定の概要	3
データ	3
ネットワークフローレコード	3
暗号化トラフィック分析 フローレコード	4
拡張 NetFlow 受信の設定	4
センサーインストールファイルの最新バージョンのダウンロード:	4
拡張 NetFlow テレメトリを送信するためのセンサーの設定:	5
Sensorのヘルスステータスの確認	5
センサーのヘルスステータスの確認:	5
拡張 NetFlow - 関連する検知機能	6
暗号化されたトラフィックレポート	6
暗号化トラフィック分析 レポートのフィールド	6
暗号化トラフィックレポートの使用	7
暗号化トラフィックレポートの表示:	7
暗号化トラフィックレポートに表示するデータの更新:	7
送信元エンティティの詳細の表示:	7
宛先エンティティの詳細の表示:	7
情報を含むカンマ区切りファイルのダウンロード:	8
その他のリソースおよびサポート	9
変更履歴	10

拡張 NetFlow 向け設定の概要

最新の Cisco スイッチやルータには、拡張 NetFlow のエクスポートが暗号化トラフィック分析機能の一部として備わっています。このテレメトリを収集するように Cisco Secure Cloud Analytics (旧 Stealthwatch Cloud) を設定することで、新しいタイプの観測およびアラート機能を実現します。詳細については、[暗号化トラフィック分析ホワイトペーパー](#)を参照してください。

ネットワークフローデータやテレメトリをクラウドに送信するために、追加のライセンスは必要ありません。

データ

2つのカテゴリのデータが HTTPS 経由でクラウドに送信され、暗号化された状態で保存されます。

- ネットワークフローレコード
- スイッチとルータで暗号化トラフィック分析を有効にし、レコードを送信するように Cisco Secure Cloud Analytics センサー (旧 Stealthwatch Cloud センサー) を設定している場合の暗号化トラフィック分析レコード

ネットワークフローレコード

ネットワークフローレコードには以下のデータが含まれます。

<ul style="list-style-type: none"> • ホスト エンドポイントの IP アドレス 	<ul style="list-style-type: none"> • 開始時刻 	<ul style="list-style-type: none"> • 最終アクティブ時刻
<ul style="list-style-type: none"> • TCP ポートまたは UDP ポート 	<ul style="list-style-type: none"> • ポート範囲 	<ul style="list-style-type: none"> • 自律システム番号
<ul style="list-style-type: none"> • mac アドレス 	<ul style="list-style-type: none"> • グループ ID 	<ul style="list-style-type: none"> • VM ID
<ul style="list-style-type: none"> • プロトコル データ* 	<ul style="list-style-type: none"> • SYN パケット数 	<ul style="list-style-type: none"> • RST パケット数
<ul style="list-style-type: none"> • 期間ごとの送信時のバイトおよびパケットの数 	<ul style="list-style-type: none"> • TrustSec セキュリティグループタグの ID と名前 	<ul style="list-style-type: none"> • フロー開始以降のバイトとパケットの合計数
<ul style="list-style-type: none"> • FIN パケット数 	<ul style="list-style-type: none"> • 既知のサービス ポート 	<ul style="list-style-type: none"> • プロトコル
<ul style="list-style-type: none"> • フロー ID 	<ul style="list-style-type: none"> • アプリケーション ID 	<ul style="list-style-type: none"> • パケットシェーパードアプリケーション ID
<ul style="list-style-type: none"> • サービス ID 	<ul style="list-style-type: none"> • センサー アプリケーション ID 	<ul style="list-style-type: none"> • NBAR アプリケーション ID
<ul style="list-style-type: none"> • Palo Alto アプリケーション ID 	<ul style="list-style-type: none"> • VLAN ID (Admin. VLAN ID) 	<ul style="list-style-type: none"> • 接続数
<ul style="list-style-type: none"> • ユーザ名 	<ul style="list-style-type: none"> • 再送信数 	<ul style="list-style-type: none"> • サーバ応答時間
<ul style="list-style-type: none"> • MPLS ラベル 	<ul style="list-style-type: none"> • エクスポートのリスト 	<ul style="list-style-type: none"> • フローシーケンス番号

• ラウンドトリップ時間	• センサー IPアドレス	• SVRD メトリック
--------------	---------------	--------------

* プロトコルデータフィールドには、URL、SSL 証明書、ヘッダーデータ用の特殊文字などのその他の情報が含まれます。

暗号化トラフィック分析 フローレコード

暗号化トラフィック分析フローレコードは、スイッチまたはルータで暗号化トラフィック分析を有効にし、拡張 NetFlow を収集するようにセンサーを設定している場合にのみ送信されます。暗号化トラフィック分析の詳細については、[暗号化トラフィック分析 のホワイトペーパー](#)および [暗号化トラフィック分析 導入ガイド](#)を参照してください。

暗号化トラフィック分析 フローレコードには以下のデータが含まれます。

• 初期データパケット (IDP)*	• パケットの長さや時間のシーケンス (SPLT)	• Transport Layer Security (TLS) バージョン
• TLS セッション UD	• 選択した暗号スイート	

* 初期データパケット (IDP)には、サーバ名表示 (SNI)、プロトコルバージョン、提供および選択された暗号スイートと HTTP ヘッダーフィールド (暗号化されていない HTTP トラフィックの場合) など、プロトコル関連のデータとヘッダーがほとんど含まれています。HTTPS/HTTP 以外のプロトコルの場合は、クライアント/サーバ通信の最初の 1500 バイトのプロトコルヘッダーが含まれています (通常は、データの残りの部分を復号することなく、プロトコルレベルで暗号化されます)。

拡張 NetFlow 受信の設定

センサーのバージョン 4.0 以降を導入すると、拡張 NetFlow テレメトリを収集するように設定できます。これにより、新しいタイプの観測とアラートが可能になります。暗号化トラフィック分析テレメトリエクスポートの設定方法については、[暗号化トラフィック分析 導入ガイド](#)を参照してください。

センサー Web UI から Secure Cloud Analytics のインストールファイルの最新バージョンをダウンロードします。センサー導入の詳細については、<https://ebooks.cisco.com/story/swc-sensor-install.html> を参照してください。

センサーインストールファイルの最新バージョンのダウンロード:

はじめる前に

- Secure Cloud Analytics Web UI にログインします。

手順

1. ? (ヘルプ) アイコン > [Sensor のインストール (Sensor Install)] を選択します。
2. ダウンロードボタンをクリックして、センサーの最新バージョンの .iso ファイルをダウンロードします。

次の作業

- <https://ebooks.cisco.com/story/swc-sensor-install.html> を参照してセンサーを導入します。

センサーを導入後、Secure Cloud Analytics Web UI にログインして、センサーが使用するよう設定されているポートを確認し、別のポートを使用して拡張 NetFlow テレメトリをクラウドに送信するようにセンサーを設定できます。

拡張 NetFlow テレメトリを送信するためのセンサーの設定:

はじめる前に

- センサーの IP アドレスにテレメトリをエクスポートするように暗号化トラフィック分析対応デバイスを設定します。



Flexible NetFlow の宛先 UDP ポートとは異なる宛先 UDP ポートを使用するように拡張 NetFlow を設定することをお勧めします。たとえば、拡張 NetFlow にはポート 2055/UDP を設定し、Flexible NetFlow にはポート 9995/UDP を設定します。

- Secure Cloud Analytics Web UI にログインします。

手順

1. (クラウド)アイコン > [Sensor (Sensors)] を選択して、Sensor リストを表示します。
2. 設定するセンサーについて、[設定の変更 (Change Settings)] をクリックします。
3. [NetFlow/IPFIX] タブを選択します。特に (Flexible) NetFlow で使用するポートのリストに注意してください。これらのポートを拡張 NetFlow 用に設定しないでください。
4. [新しいプローブの追加 (Add New Probe)] をクリックします。
5. [プローブタイプ (Probe Type)] で拡張 NetFlow (et-analytics) を選択します。
6. 暗号化トラフィック分析対応デバイス用に設定した UDP ポートを入力します。
設定する UDP ポートが、センサーの設定で Flexible NetFlow や IPFIX 用にも設定されていないことを確認してください。そのように設定されている場合、拡張 NetFlow 用に設定したポートが拡張 NetFlow 専用になるように設定を更新してください。
7. [プロトコル (Protocol)] で UDP を選択します。
8. [送信元 (Source)] で Standard を選択します。
9. [保存 (Save)] をクリックします。

Sensor のヘルスステータスの確認

Sensor リストページからセンサーのヘルスステータスをチェックすることで、センサーが正しく設定されているかを確認できます。


センサーのヘルスステータスの確認:

はじめる前に

- Secure Cloud Analytics Web UI にログインします。

手順

1. (クラウド)アイコン > [Sensor (Sensors)] を選択して、Sensor リストを表示します。

2. 設定したセンサーを見つけます。センサーに緑色の上矢印  (クラウド) アイコンが表示されている場合、センサーは正しく設定されています。表示されていない場合は、センサーの設定を確認します。

拡張 NetFlow – 関連する検知機能

Secure Cloud Analytics は拡張 NetFlow テレメトリに基づいて、以下をベースとした脅威を検出できます。

- DNSドメイン名クエリ
- HTTPS リクエスト内のホスト名
- HTTP リクエスト内の URL パターン

Secure Cloud Analytics テレメトリが既知の脅威と一致すると、観測結果とアラートが生成されます。

暗号化されたトラフィックレポート

暗号化トラフィックレポートには、暗号化トラフィック分析に基づき、送信元および宛先エンティティ、暗号化方式の詳細など、システムがモニターした暗号化トラフィックに関する詳細情報が表示されます。デフォルトでは、過去 24 時間の情報が表示されます。表示される情報の期間を変更したり、表示される暗号化接続をフィルタリングしたりできます。暗号化された接続に関する詳細を含むカンマ区切り値 (CSV) ファイルをダウンロードすることもできます。

このモデルを実装するには、拡張 NetFlow データがクラウドに送られるようにセンサーを設定する必要があります。詳細については、『[Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#)』を参照してください。

暗号化トラフィック分析 レポートのフィールド

フィールド	説明
時刻 (Time)	システムがセッションを検出したタイムスタンプ。
IP	セッションを開始した IP アドレス。
ポート (Port)	接続元 IP アドレスがトラフィックの送信に使用したポート。
リモート IP (Remote IP)	接続元 IP アドレスがセッションを確立した IP。
リモート ポート (Remote Port)	リモート IP アドレスがトラフィックの送信に使用したポート。
接続ポート (Connected Port)	接続された IP アドレスがトラフィックの送信に使用したポート。
暗号化プロトコル (Encryption Protocol)	暗号化されたセッションプロトコル。

暗号化キー交換 (Encryption Key Exchange)	暗号化された接続を確立するために使用された暗号化キーの交換方式。
暗号化キー長 (Encryption Key Length)	交換される暗号化キーの長さ(ビット単位)。
暗号化アルゴリズム (Encryption Algorithm)	接続を保護するために使用された暗号化アルゴリズム。
暗号化 MAC (Encryption MAC)	接続の認証に使用された暗号化メッセージの認証コード。

暗号化トラフィックレポートの使用

暗号化トラフィックレポートの表示:

手順

- [モデル (Models)] > [暗号化トラフィック分析] を選択します。

暗号化トラフィックレポートに表示するデータの更新:

手順

1. フィルターペインを展開します。
2. 接続元のホストでフィルタリングする場合は、接続元 IP アドレスを入力します。
3. 接続先のホストでフィルタリングする場合は、リモート IP アドレスを入力します。
4. 接続元のホストのポートでフィルタリングする場合は、接続元のポートを入力します。
5. 接続先のホストのポートでフィルタリングする場合は、リモートポートを入力します。
6. 暗号化プロトコルでフィルタリングする場合は、ドロップダウンから [プロトコル (Protocol)] を選択します。
7. 使用する暗号化アルゴリズムでフィルタリングする場合は、アルゴリズムを入力します。
8. メッセージ認証コードでフィルタリングする場合は、ドロップダウンから [MAC] を選択します。
9. 暗号化キー交換方式でフィルタリングする場合は、キー交換方式を入力します。
10. 暗号化キーの長さでフィルタリングする場合は、最小および最大のキーの長さを入力します。
11. 新しい開始日と開始時刻を入力します。
12. 新しい終了日と終了時刻を入力します。
13. [更新 (Update)] をクリックします。

送信元エンティティの詳細の表示:

手順

(missing or bad snippet)

宛先エンティティの詳細の表示:

手順

(missing or bad snippet)

情報を含むカンマ区切りファイルのダウンロード: 手順

- ダウンロードする表の [CSV] をクリックします。

その他のリソースおよびサポート

さらにサポートが必要な場合は、support@obsrvbl.com まで電子メールでお問い合わせください。

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、<https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> を参照してください。
- 60 日間の無料トライアルに登録するには、<https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> にアクセスしてください。
- ドキュメントリソースについては、<https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> を参照してください。
- Secure Cloud Analytics 無料トライアルのガイドなど、インストールおよび設定ガイドについては、<https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> を参照してください。

変更履歴

リビジョン	改訂日	説明
1.0	2019年10月8日	最初のバージョン。
1.1	2019年10月24日	その他の更新および訂正。
1.2	2019年11月5日	センサーの設定手順を更新。
2.0	2021年11月3日	製品のブランド名を更新。

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)