Cisco Secure Cloud Analytics

拡張 NetFlow 設定ガイド

目次

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。

• ホスト エンドポイントの IP アドレス	• 開始時刻	• 最終アクティブ時刻
• TCP ポートまたは UDP ポート	• ポート範囲	• 自律システム番号
• mac アドレス	• グループ ID	• VM ID
• プロトコル データ*	• SYN パケット数	• RST パケット数
• 期間ごとの送信時のバイトおよびパケットの数	• TrustSec セキュリティ グループ タグの ID と名前	• フロー開始以降のバイトとパケットの合計数
• FIN パケット数	• 既知のサービス ポート	• プロトコル
• フロー ID	• アプリケーション ID	• パケット シェーパー アプリケーション ID
• サービス ID	• センサーアプリケーション ID	• NBAR アプリケーション ID
• Palo Alto アプリケーション ID	• VLAN ID（Admin. VLAN ID）	• 接続数
• ユーザ名	• 再送信数	• サーバ応答時間
• MPLS ラベル	• エクスポータのリスト	• 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構成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）*	• パケットの長さと時間のシーケンス（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 以降を展開すると、拡張 NetFlow テレメトリを収集するように構成できます。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タ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。

Secure Cloud Analytics Web UI から最新バージョンのセンサーのインストールファイルをダウンロードします。センサセンサーの展開の詳細については、https://ebooks.cisco.com/story/swc-sensor-install.html を参照してください

最新バージョンのセンサーのインストールファイルをダウンロードします。

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 > [センサーのインストール（Sensor Install）]**。
2. ダウンロードボタンをクリックして最新バージョンのセンサー .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展開します。

センサーを展開した後、Secure Cloud Analytics Web UI にログインしてセンサーが使用するように構成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渡すようにセンサーを構成できます。

拡張 NetFlow テレメトリを渡すようにセンサーを構成します。

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 対応デバイスを構成します。

  > 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 > [センサー(Sensors)] を選択してセンサー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。

   構成する UDP ポートがセンサーの構成で Flexible NetFlow や IPFIX 用にも構成されていないことを確認します。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。

センサーの正常性ステータスの確認

[センサーリスト(Sensor List)] ページでセンサーの正常性ステータスを確認することでセンサーの構成を確認できます。

センサーの正常性ステータスを確認します。

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 > [センサー(Sensors)] を選択してセンサーリストを表示します。

2. 構成されたセンサーを見つけます。(クラウド)アイコン に緑色の上矢印が表示されている場合は、センサーが正しく設定されています。それ以外の場合は、センサー構成を確認してください。

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。

このモデルを入力するには、拡張 NetFlow データをクラウドに渡す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	暗号化された接続を確立するために使用された暗号化

Exchange)	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

1. エンティティに関連するすべてのアラートを表示するには、IP アドレスまたはホスト名のドロップダウンから、[アラート(Alerts)] を選択します。
2. エンティティに関連するすべてのアラートを表示するには、IP アドレスまたはホスト名のドロップダウンから、[観測内容(Observations)] を選択します。

3. デバイスに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[デバイス(Device)] を選択します。
4. このエンティティに関連するセッショントラフィックを表示するには、IP アドレスまたはホスト名のドロップダウンから、[セッショントラフィック(Session Traffic)] を選択します。
5. IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから、[コピー(Copy)] を選択します。
6. この IP に基づいて他のシスコ製品でアクションを実行するには、SecureX の統合に応じて、[SecureX でさらに拡張(More with SecureX)] を展開します。

> この機能を有効にするには、SecureX セキュリティリボンにログインする必要があります。

宛先エンティティの詳細の表示:

手順

1. このエンティティの最近のトラフィック情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[IPトラフィック(IP Traffic)] を選択します。
2. このエンティティの最近のセッショントラフィック情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[セッショントラフィック(Session Traffic)] を選択します。
3. AbuseIPDB のウェブサイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[AbuseIPDB] を選択します。
4. Cisco Umbrella のウェブサイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[Cisco Umbrella] を選択します。
5. Google でこの IP アドレスを検索するには、IP アドレスまたはホスト名のドロップダウンから、[Google検索(Google Search)] を選択します。
6. Talos のウェブサイト上で情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[Talos Intelligence] を選択します。
7. このエンティティをウォッチリストに追加するには、IP アドレスまたはホスト名のドロップダウンから、[IPをウォッチリストに追加(Add IP to watchlist)] を選択します。
8. 前月のこのエンティティのトラフィックを検索するには、IP アドレスまたはホスト名のドロップダウンから、[複数日のIPを検索(Find IP on multiple days)] を選択します。
9. IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから、[コピー(Copy)] を選択します。
10. この IP に基づいて他のシスコ製品でアクションを実行するには、SecureX の統合に応じて、[SecureX でさらに拡張(More with SecureX)] を展開します。

> この機能を有効にするには、SecureX セキュリティリボンにログインする必要があります。

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。

関連リソース

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 初期導入ガイドなど、インストールおよびコンフィギュレーション 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。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- Secure Cloud Analytics 無料トライアルの試用時に電子メールでケースを開く場合：
  swatchc-support@cisco.com

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。
2.1	2022 年 8 月 4 日	「サポートへの問い合わせ」セクションを追加。

著作権情報