Cisco Secure Network Analytics

グローバル脅威アラート コンフィギュレーション ガイド 7.4

目次

はじめに

シスコグローバル脅威アラート（旧 Cognitive Intelligence） は、疑わしい Web トラフィックや Cisco Secure Network Analytics（旧 Stealthwatch）フローレコードを迅速に検出し、環境内でのプレゼンス確立の試みや、すでに発生中の攻撃に対処します。Secure Network Analytics が Secure Network Analytics で有効になると、分析のためにフローレコードがグローバル脅威アラート クラウドに送信されます。デフォルトでは、グローバル脅威アラートは、内外のホストグループトラフィックおよび DNS 要求の Secure Network Analytics フローレコードを処理します。内部トラフィックを監視する追加のホストグループを指定できます。また、グローバル脅威アラートは Cisco 暗号化トラフィック分析を使用して暗号化されたトラフィックの悪意のあるパターンを検出します。

グローバル脅威アラートは Secure Network Analytics と連携して、フローレコードとネットワークアドレス変換（NAT）を分析します。Secure Network Analytics フローレコードをグローバル脅威アラートに送信するために追加のライセンスは必要ありませんが、Web トラフィックデータを Secure Network Analytics からグローバル脅威アラートに送信するには、インターネット境界 NAT データが必要です。これらの製品に関する詳細情報へのリンクについては、このドキュメントの最後にある「**関連資料**」を参照してください。

- グローバル脅威アラートは Amazon Web Services（AWS）クラウドに移行し、URL と IP アドレスが新しくなりました。詳細については、次のフィールド通知を参照してください。
  フィールド通知：2018 年 5 月
  フィールド通知：2018 年 10 月

サポート

グローバル脅威アラートは、スマートライセンス予約が使用されている場合はサポートされません。

- マネージャ（旧 StealthWatch Management Console）およびFlow Collectorは、プロキシサーバー経由でインターネットに接続するように設定できます。詳細については、「**プロキシ設定**」を参照してください。
- グローバル脅威アラートは、そのドメインに関連付けられたフローコレクタが有効になっている限り、各ドメインを分析します。生成されたアラートのリストは、すべてのドメインから取得されたデータの集約です。ドメインごとに分割されていません。
- 特定のクライアント IP アドレスが複数のドメインに存在する場合、グローバル脅威アラートは、該当するすべてのドメインにわたってこの IP アドレスのすべてのアラートを識別し、これらのアラートを結果の同じグループに配置します。ただし、ホストグループのデータはフローコレクタごとに個別に収集されるため、グローバル脅威アラートダッシュボードで結果をホストグループでフィルタリングできます（メインメニューから [ダッシュボード（Dashboards）] > [グローバル脅威アラート（Global Threat Alerts）] を選択します）。
- グローバル脅威アラートは Flow Collector（sFlow） ではサポートされていません。
- グローバル脅威アラートは FIPS 暗号化ライブラリが有効になっている場合、使用できません。

暗号化トラフィック分析サポート

グローバル脅威アラートは暗号化トラフィック分析対応のスイッチとルータがある場合、暗号化トラフィック分析情報のみ検出できます。Secure Network Analytics と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の導入ガイドを参照してください。

ユーザとデータロール

次のユーザが	次のデータロールを使用する場合	アクセス可能なもの
プライマリ Admin（Primary Admin）	すべてのデータ（読み取りおよび書き込み）	• グローバル脅威アラート ダッシュボード • グローバル脅威アラート コンポーネント
パワーアナリスト（Power Analyst）		
設定マネージャ（Configuration Manager）	すべてのデータ（読み取り専用）*	• グローバル脅威アラート ダッシュボード
アナリスト（Analyst）		

* 設定マネージャ（Configuration Manager）とアナリスト（Analyst）のデータロールを変更すれば、グローバル脅威アラート へのフルアクセスを付与できます。詳細については、ユーザ管理の設定に関するヘルプトピックを参照してください。

データ

次の 2 つのカテゴリのデータがダブリンの AWS データセンターに送信されます。

- 次の条件のいずれかが満たされた場合の Secure Network Analytics フローレコード:
  - 内部/外部ホスト グループのトラフィックのレコード
  - 特定の内部ホスト グループのトラフィックのレコード(**内部ホスト**)
  - サーバポートが 53 の場合の DNS 要求レコード
  - 暗号化トラフィック分析対応のスイッチとルーターがある場合は、暗号化トラフィック分析を記録
- Web ログデータ(Secure Network Analytics プロキシログがある場合)

Secure Network Analytics フローレコード

Secure Network Analytics 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
- TCP ポートまたは UDP ポート
- mac アドレス
- プロトコル データ*
- 期間ごとの送信時のバイトおよびパケットの数
- FIN パケット数
- フロー ID
- サービス ID
- Palo Alto アプリケーション ID
- ユーザ名
- MPLS ラベル
- ラウンド トリップ時間
- 開始時刻
- ポート範囲
- グループ ID
- SYN パケット数
- TrustSec セキュリティ グループ タグの ID と名前
- 既知のサービス ポート
- アプリケーション ID
- フローセンサー アプリケーション ID
- VLAN ID(Admin. VLAN ID)
- 再送信数
- エクスポータのリスト
- Flow Collector IPアドレス
- 最終アクティブ時刻
- 自律システム番号
- VM ID
- RST パケット数
- フロー開始以降のバイトとパケットの合計数
- プロトコル
- パケット シェーパー アプリケーション ID
- NBAR アプリケーション ID
- 接続数
- サーバ応答時間
- フロー シーケンス番号
- 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、暗号化トラフィック分析が有効になっているスイッチとルータがある場合にのみ送信されます。Secure Network Analytics と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の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）*
- TLS セッション UD
- パケットの長さと時間のシーケンス（SPLT）
- 選択した暗号スイート
- Transport Layer Security（TLS）バージョン

* 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）。

Web ログ データ

Web ログデータの目的の 1 つは、NAT を介してルーティング不可能な内部 IP とルーティング可能な外部パブリック IP の間の変換を提供することです。

> Secure Network Analytics でサポートされているプロキシログ設定については、『Cisco Secure Network Analytics Stealthwatch proxy log Configuration Guide』を参照してください。

Web ログ データには以下が含まれます。

- タイムスタンプ
- サーバ IP アドレス
- クライアント TCP ポート
- クライアントからサーバに転送されたバイト数
- HTTP Referrer ヘッダー
- user-agent 文字列
- 経過時間
- クライアント ユーザ名（オプション）
- サーバ TCP ポート
- サーバからクライアントに転送されたバイト数
- HTTP 応答ステータスコード
- 応答 MIME タイプまたはコンテンツ タイプ
- クライアント IP アドレス
- サーバ名
- 要求された URL/URI
- HTTP 要求メソッド
- HTTP Location ヘッダー
- Web セキュリティ プロキシによって実行されるアクション

マネージャの設定

ダッシュボード コンポーネント

マネージャでグローバル脅威アラート コンポーネントを構成するには、次の手順を実行します。

すべてのアプライアンスは、グローバル脅威アラートに接続するために NTP サーバーを使用して同期されたクロックを持っている必要があります。

デュアルマネージャのペアでは、構成後にセカンダリマネージャはグローバル脅威アラートに接続しません。これは、Flow Collector がデータを受信することを妨げず、プライマリマネージャがグローバル脅威アラートに接続し、ウィジェットを適切に表示します。プライマリマネージャに障害が発生すると、セカンダリマネージャがグローバル脅威アラートに接続し、ウィジェットを表示します。元のプライマリマネージャが稼働状態に戻ると、両方のマネージャがグローバル脅威アラートに正常に接続します。

少なくとも 1 つのマネージャがインターネットにアクセスする必要があります。プロキシ設定も必要な場合は、「**プロキシ設定**」で詳細を確認してください。

1. マネージャから次の IP アドレスおよびポート 443 への通信を許可するようにネットワーク ファイアウォールを構成します。

サービス	URL エイリアス	サービス IP
CTA 公開ランディングページ	https://cta.eu.amp.cisco.com/ https://cognitive.cisco.com/ （エイリアス）	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA ログインページ	https://cta.eu.amp.cisco.com/ https://td.cloudsec.sco.cisco.com/CWSP/ （エイリアス）	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA TAXII サービス	https://cta.eu.amp.cisco.com/taxii https://taxii.cloudsec.sco.cisco.com （エイリアス）	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105

パブリック DNS が許可されていない場合は、マネージャでローカルに解決方法を設定する必要があります。

2. Manager にログインします。
3. ⚙ ([グローバル設定(Global Settings)]) アイコン をクリックします。[集中管理(Central Management)] を選択します。
4. マネージャの [アクション(Actions)] 列の下にある ••• ([省略記号(Ellipsis)]) アイコン をクリックします。[アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
5. [全般(General)] タブをクリックします。
6. [外部サービス(External Services)] で [グローバル脅威アラートの有効化(Enable Global Threat Alerts)] チェックボックスをオンにして、[セキュリティ分析(Security Insight)] ダッシュボードおよびホストレポートの グローバル脅威アラート コンポーネントを有効にします。
7. (省略可)グローバル脅威アラートがクラウドから自動的にアップデートを送信できるようにするには、[自動更新(Automatic Updates)] チェックボックスをオンにします。

   自動更新により、グローバル脅威アラート クラウドのセキュリティ修正と小規模な機能拡張のほとんどが実行されます。これらの更新は、通常の Secure Network Analytics リリースプロセスでも利用可能です。いつでもこのオプションを無効にして、クラウドからの自動更新を停止できます。マネージャで自動更新を有効にした場合は、Flow Collector でも有効にする必要があります。

8. [設定の適用(Apply settings)] をクリックします。

   サービスが更新され、Security Insight ダッシュボードとホストレポートのグローバル脅威アラート コンポーネントが表示されるまでに数分かかります。

9. (省略可)インターネットプロキシをアップロードするには、[ネットワークサービス(Network Services)] に移動します。[インターネットプロキシ(Internet Proxy)] セクションまでスクロールダウンし、[有効(Enable)] チェックボックスをオンにします。フォームに入力してから、[設定の適用(Apply Settings)] をクリックします。

内部ホスト

デフォルトでは、グローバル脅威アラートは、内外のホストグループトラフィックおよび DNS 要求の Secure Network Analytics フローレコードを処理します。分析用にクラウドに送信するデータを追加するには、Secure Network Analytics フローレコードを送信する内部ホストグループを設定します。特定のホストグループをグローバル脅威アラート モニタリングに追加する方法は、企業の内部サーバー(メールサーバー、ファイルサーバー、Web サーバー、認証サーバーなど)に使用されます。これらのサーバーにエンドユーザーからのトラフィックを追加すると、該当のデバイスで実行されているマルウェアによって悪用される可能性がある、データの露出の可視性を改善できます。データを送信するホスト グループをすべて選択するのではなく、内部サーバを表すホスト グループのみを選択してください。

グローバル脅威アラートが内部ホストのトラフィックをモニターできるようにするには、次の手順を実行します。

1. Manager にログインします。
2. [設定(Configure)] > [ホストグループ管理(Host Group Management)] に移動します。
3. 該当する内部ホストグループをクリックし、[グローバル脅威アラート にフローを送信する(Send Flow to Global Threat Alerts)] チェックボックスをオンにします。

この機能により、選択した親ホスト グループの下にあるすべてのホスト グループのトラフィックのモニタリングが有効になります。潜在的なパフォーマンスの問題を避けるため、このオプションは子ホスト グループでのみ有効にすることをお勧めします。

4. [保存(Save)]をクリックします。

Flow Collector の設定

Flow Collector（NetFlow）でグローバル脅威アラート コンポーネントを構成するには、次の手順を実行します。

> すべてのアプライアンスは、グローバル脅威アラートに接続するために NTP サーバーを使用して同期されたクロックを持っている必要があります。

> 正確な結果を得るには、各 Flow Collector でグローバル脅威アラートを設定する必要があります。

> 設定後、グローバル脅威アラート エンジンがネットワークの動作を学習するのに 2 日間かかります。

1. Flow Collector から次の IP アドレスおよびポート 443 への通信を許可するように、ネットワークのファイアウォールを設定します。

サービス	URL エイリアス	サービス IP
CTA 公開ランディングページ	https://cta.eu.amp.cisco.com/ https://cognitive.cisco.com/（エイリアス）	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA ログインページ	https://cta.eu.amp.cisco.com/ https://td.cloudsec.sco.cisco.com/CWSP/（エイリアス）	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA TAXII サービス	https://cta.eu.amp.cisco.com/taxii https://taxii.cloudsec.sco.cisco.com（エイリアス）	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA データ取り込みサービス	https://etr.cta.eu.amp.cisco.com https://etr.cloudsec.sco.cisco.com（エイリアス）	AWS EIP: *34.251.210.21 • 34.255.162.33 • 54.194.49.205

> パブリック DNS が許可されていない場合は、Flow Collector でローカルに解決方法を設定する必要があります。

2. マネージャにログインします。
3. ⚙ ([グローバル設定(Global Settings)]) アイコン をクリックします。[集中管理(Central Management)] を選択します。
4. Flow Collector(NetFlow) の [アクション(Actions)] 列の下にある ••• ([省略記号(Ellipsis)]) アイコン をクリックします。[アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
5. [全般(General)] タブをクリックします。
6. [外部サービス(External Services)] で [グローバル脅威アラートの有効化(Enable Global Threat Alerts)] チェックボックスをオンにして、Flow Collector から グローバル脅威アラート エンジンへのデータの送信を有効にします。
7. (省略可)グローバル脅威アラートがクラウドから自動的にアップデートを送信できるようにするには、[自動更新(Automatic Updates)] チェックボックスをオンにします。

   自動更新により、グローバル脅威アラート クラウドのセキュリティ修正と小規模な機能拡張のほとんどが実行されます。これらの更新は、通常の Secure Network Analytics リリースプロセスでも利用可能です。いつでもこのオプションを無効にして、クラウドからの自動更新を停止できます。フローコレクタで自動更新を有効にした場合は、マネージャでも有効にする必要があります。

8. [設定の適用(Apply settings)] をクリックします。

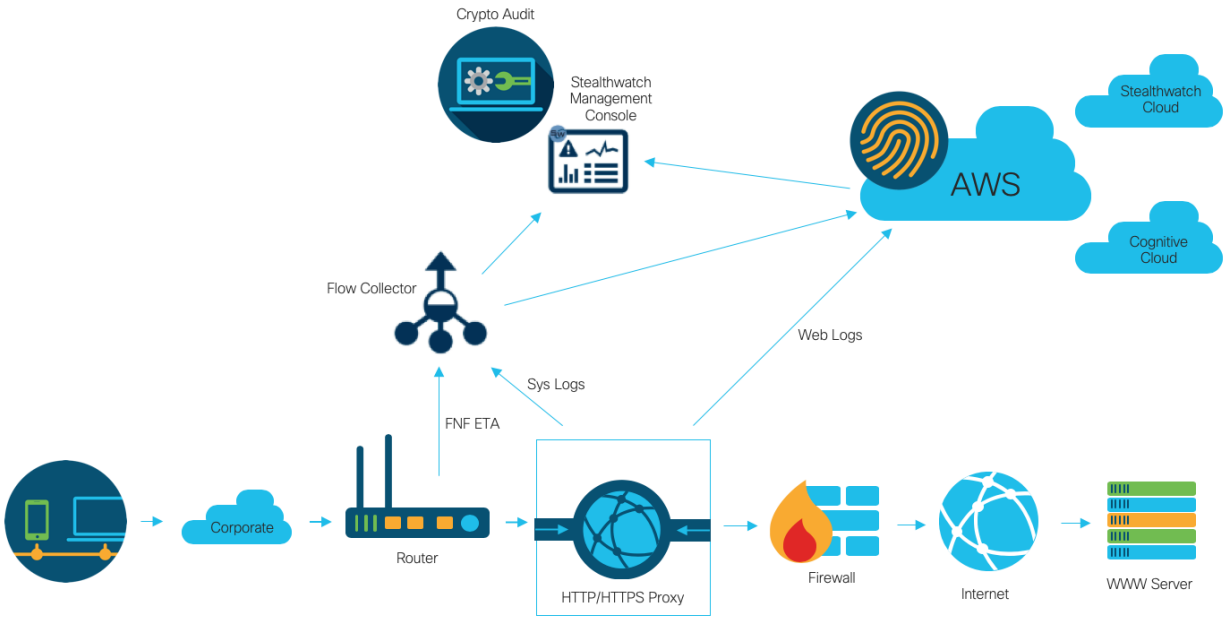
プロキシ設定

これを実現するには、プロキシサーバーを介してインターネットに接続するようにマネージャと Flow Collector を構成します。グローバル脅威アラートは SSL インスペクションが無効になっている HTTP/HTTPS プロキシをサポートしています。Secure Network Analyticsは SOCKS プロキシをサポートしていません。

Web プロキシの設定方法の詳細については、このドキュメントのセクション「**マネージャの設定**」を参照してください。プロキシログの設定の詳細については、『Cisco Secure Network Analyticsプロキシログの設定』を参照してください。

セットアップの設定については、次の図を参照してください。

> この設定では、WSA のプロキシを透過モードにする必要があります。詳細については、「WSA を設定し、グローバル脅威アラート システムにログファイルをアップロードする」を参照してください。



次の場合、プロキシを使用してグローバル脅威アラートの最適な結果を得ることができます。

- Flow Collector は、プロキシの前にフローを収集します。
- プロキシログはクラウドに直接送信されます。

次の場合、プロキシを使用して Secure Network Analytics の最適な結果を得ることができます。

- プロキシログは次の宛先に直接送信されます：Flow Collector
- 次を有効にします：暗号化トラフィック分析

プロキシをクラウドに直接接続する方法の詳細については、次を参照してください。

Blue Coat ProxySG を設定し、グローバル脅威アラート システムにログファイルをアップロードする

McAfee Web ゲートウェイを設定し、グローバル脅威アラート システムにログファイルをアップロードする

WSA を設定し、グローバル脅威アラート システムにログファイルをアップロードする

検証

Docker サービス

グローバル脅威アラートが適切に設定されていることを確認するには、次の手順を実行します。

> グローバル脅威アラート を無効にするには、[一元管理（Central Manager）] > [アプライアンスの編集（Edit Appliance）] > [全般（General）] に移動し、それぞれの マネージャと Flow Collector（NetFlow） の [グローバル脅威アラートの有効化（Enable Global Threat Alerts）] チェックボックスをオフにします。

1. グローバル脅威アラートがマネージャと Flow Collector で有効になっていることを確認します。
2. グローバル脅威アラート コンポーネントがセキュリティ インサイト ダッシュボードおよびホストレポートに表示されていることを確認します。
3. ナビゲーションメニューから、[ダッシュボード（Dashboard）] > グローバル脅威アラートをクリックします。グローバル脅威アラート ダッシュボードページが開きます。ページの右上にあるメニューから [デバイスアカウント（Device Accounts）] をクリックします。設定されている各 Flow Collector のアカウントでデータがアップロードされていて、準備ステータスになっていることを確認します。

暗号化トラフィック分析統合

グローバル脅威アラートは 暗号化トラフィック分析ソリューション内にマルウェア検出機能を実装します。暗号化トラフィック分析ソリューションが正しく設定されていることを確認するために、グローバル脅威アラートで特定のテストサイトドメインを使用して暗号化トラフィック分析テストインシデントを生成できます。これらのテストインシデントを生成するには、HTTPS セッションが 暗号化トラフィック分析対応スイッチおよびルータを通過するホストを使用して、次のテストサイトのいずれかを参照します。

- マルウェア：https://examplemalwaredomain.com
- ボットネット：https://examplebotnetdomain.com
- フィッシング：https://internetbadguys.com

> 最初は検出結果にリスク レーティング 5 と表示されます。上記の複数の URL にアクセスしたり、同じ URL に繰り返しアクセスしたりといった不正または反復的な動作が行われると、リスク レーティングが増大する可能性があります。

- TOR 検出：TOR ブラウザをダウンロードしてインストールし（https://www.torproject.org/projects/torbrowser.html.en）、いくつかのウェブサイトにアクセスしてください。
- TOR 検出は、リスクレーティング 4 の「TORリレー（TOR relay）」または「潜在的に望ましくないアプリケーション（Possibly Unwanted Application）」と表示されます。

既知の問題

このセクションでは、このリリースに存在する既知の問題（バグ）について概要を示します。可能な場合には、回避策も示しています。参照用に問題番号が示されています。

問題番号	説明	回避策
CHOPIN-25314	Secure Network Analytics ユーザーの権限が昇格または降格された場合（例：読み取り専用から読み取り/書き込みへ、またはその逆）、グローバル脅威アラートに変更が伝わるまでに最大 30 分かかります。	現在使用可能なものはありません。
SWD-13834	設定の復元を実行すると、グローバル脅威アラートが無効になります。	これを克服するには、バックアップの復元プロセス後に手動でグローバル脅威アラートを有効にします。
NA	ユーザーが複数の Secure Network Analytics システムにログインすると、グローバル脅威アラート内の 2 番目のシステムにログインできなくなります。	この問題を解決するには、次の手順に従います。 • 最初のログインが期限切れになるまで 30 分待機します。 • 最初のシステム上で グローバル脅威アラート からログアウトします。

関連資料

- グローバル脅威アラートの詳細については、製品の Web サイト（https://cognitive.cisco.com）にアクセスするか、http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011110.html にある製品マニュアルを参照してください。
- すべてのシスコ クラウド製品のクラウド利用規約とオファーの説明については、http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html を参照してください。
- Cisco Universal Cloud 契約については、http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf を参照してください。
- オファー全般については、http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/omnibus-cloud-security.pdf を参照してください。
- Secure Network Analyticsプロキシログおよび Web プロキシの詳細については、https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-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。
- シスコサポートにご連絡ください。
- 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

著作権情報