CLI および ASDM を使用した Cisco ASA と Cisco Security Analytics and Logging（SaaS）の統合

改訂：2023 年 9 月 19 日

Cisco ASA と Cisco Security Analytics and Logging（SaaS）の統合ガイド

このガイドでは、SAL（SaaS）を使用した ASA の設定方法、SAL（SaaS）でのイベントと syslog メッセージの処理方法、および CDO からのイベントの表示方法について説明します。

概要

syslog および NetFlow セキュアイベントロギング（NSEL）のイベントを外部イベントサービスに送信し、Cisco Cloud にログを保存し、Cisco Defense Orchestrator（CDO）の [Event Logging] ページで表示するように、ASA デバイスを設定できます。[Event Logging] ページでは、イベントのフィルタ処理、ダウンロード、およびセキュリティの問題のトラブルシューティングのための確認を行うことができます。このガイドでは、Adaptive Security Device Manager（ASDM）の管理対象ASAデバイスと Cisco Security Analytics and Logging (SaaS) ソリューションを統合する手順について説明します。

（注） CDO の管理対象 ASA と SAL（SaaS）の統合の詳細については、「Cisco Security Analytics and Logging for ASA Devices」を参照してください。

syslog と NSEL イベント

syslog は、ASA デバイスによって syslog サーバーに送信されるシステムログまたはイベントメッセージで、モニタリングとデバイスの問題のトラブルシューティングに使用されます。syslog メッセージには、イベントのタイプとそのシビラティ（重大度）を示すクラスと ID があります。ASA syslog メッセージの詳細については、『ASA Syslog Guide』を参照してください。

NSEL は、フロー内の重要なイベントを示すレコードだけをエクスポートする、ステートフル フロー トラッキング方式です。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。NSEL イベントには同等の syslog メッセージがあります。これらの syslog メッセージは、ファイアウォール拒否およびファイアウォール トラフィックとして CDO イベントフィルタで分類されます。Cisco ASA では、NetFlow バージョン 9 サービスがサポートされています。詳細については、『Cisco ASA NetFlow Implementation Guide』を参照してください。

（注） SWC サービスを利用するには、NSEL がデータを SAL（SaaS）に送信できるようにする必要があります。

ASA と SAL（SaaS）の統合のコンポーネント

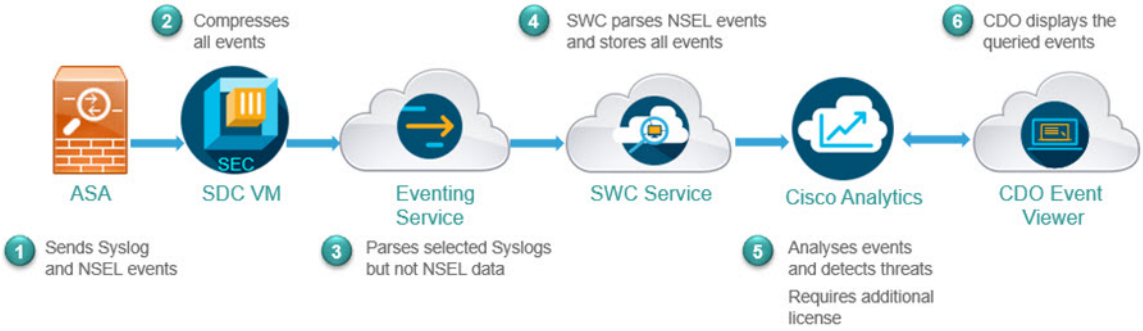
- Cisco Adaptive Security Device Manager（ASDM）：ASA デバイスを管理するグラフィカル インターフェイス ツール。
- オンプレミスの Secure Device Connector（SDC）：SDC は CDO と ASA の間の通信を処理します。オンプレミス SDC は、ネットワークのハイパーバイザにインストールされる仮想アプライアンスです。シスコが提供するイメー

ジを使用してオンプレミス SDC を作成することも、独自の VM を作成して SDC をインストールすることもできます。

- Secure Event Connector（SEC）：ASA デバイスからイベントを受信して Cisco Cloud に転送する、オンプレミスの Secure Device Connector（SDC）にインストールされるアプリケーション。
- Stealthwatch Cloud（SWC）：ネットワークから収集されたイベントの詳細な分析を提供する、クラウドベースの分析ソリューション。ネットワークトラフィックの傾向を特定し、異常な動作を調べることができます。
- Cisco Defense Orchestrator（CDO）：CDO はクラウドベースのマルチデバイスマネージャで、ローカル ASA デバイスマネージャ（具体的には ASDM）および SSH 接続と共存します。CDO アカウントを使用すると、Cisco Cloud に保存されている ASA イベントログを表示できます。追加のライセンスを使用して、CDO から、プロビジョニングされた Stealthwatch Cloud ポータルを相互起動できます。

次での ASA イベントフロー： SAL（SaaS）

統合が成功した後の SAL での ASA イベントのフローを次に示します。



1. ASA は、CDO で設定された SDC VM の SEC コンポーネントにイベント（syslog および NSEL イベント）を送信します。
2. SEC は ASA から TCP と UDP の両方の syslog を受け入れ、イベントを圧縮します。その後、イベントは Cisco Cloud に安全に転送されます。SEC は、圧縮されたイベントをクラウドベースのイベントサービスに送信します。

   （注） イベントは、データの安全な転送を確保するために圧縮されます。データサブスクリプションおよび過去の月使用量は、この圧縮データでは評価されません。これらは、使用する非圧縮データで評価されます。

3. イベントサービスは syslog イベントを解析します。NSEL データは解析しません。syslog イベントと NSEL データの両方を、Stealthwatch Cloud（SWC）ソリューションに転送します。
4. SWC は NSEL を解析し、結果を syslog イベントとともに保存します。
5. Cisco Analytics サービスは、イベントを分析し、観測結果に基づいて脅威を検出します。このサービスを利用するには、Logging Analytics and Detection ライセンスまたは Total Network Analytics and Detection ライセンスが必要です。

6. CDO イベントビューアには、フィルタ条件に基づいて Cisco Cloud に保存されているイベントが表示されます。

SAL（SaaS） 統合の要件と前提条件

要件または前提条件のタイプ	要件
ASA	Cisco Adaptive Security Device Manager（ASDM）リリース 7.0 以降。 ソフトウェアリリース 9.0 以降を実行している ASA。 アプライアンスが展開され、イベントを正常に生成している必要があります。
地域のクラウド	イベントの宛先となる地域クラウドを決定します。 イベントは、異なる地域のクラウドから表示したり、異なる地域のクラウド間で移動することはできません。
データプラン	システムに必要なクラウドストレージの容量を決定します。 ストレージ要件の計算とデータプランの購入 （5 ページ） を参照してください。
ライセンシング	• Cisco Security Analytics and Logging ライセンス：任意 ライセンスのオプションと説明については、SAL（SaaS） ライセンス （4 ページ）を参照してください。 • CDO ライセンス：追加の CDO ライセンスは必要ありません。 • Stealthwatch Cloud ライセンス：追加のライセンスは必要ありません。 • ASA ライセンス：追加のライセンスは必要ありません。 ASA のシスコ スマート ソフトウェア ライセンシングについては、『Cisco Smart Software Licensing』を参照してください。
アカウント	この統合のライセンスを購入すると、この機能をサポートする CDO テナントアカウントが提供されます。
追加の前提条件	各手順の「はじめる前に」または「前提条件」を参照してください。

SAL（SaaS） ライセンス

ライセンス	詳細
無料トライアル	30 日間の無料トライアルライセンスを取得するには、https://info.securexanalytics.com/sal-trial.html にアクセスしてください。
Logging and Troubleshooting	イベントを Cisco Cloud に保存し、CDO の Web インターフェイスを使用して、保存されたイベントを表示およびフィルタ処理します。

ライセンス	詳細
（オプション）Logging Analytics and Detection	システムは、ASA イベントに Stealthwatch Cloud の動的エンティティモデリングを適用し、行動モデリング分析を使用して Stealthwatch Cloud の観測値とアラートを生成することができます。Cisco Single Sign-On を使用して、CDO から、プロビジョニングされた Stealthwatch Cloud ポータルを相互起動できます。 SAL のライセンスを購入すると、ログを表示するための CDO テナントへのアクセスと、脅威を検出するための SWC インスタンスが提供されます。SAL のユーザーは、これらの 2 つのポータルにアクセスして SAL が提供する結果を確認するために個別の CDO ライセンスまたは SWC ライセンスを必要としません。
（オプション）Total Network Analytics and Detection	システムは、ASA イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、CDO から、プロビジョニングされた Stealthwatch Cloud ポータルを相互起動できます。 SAL のライセンスを購入すると、ログを表示するための CDO テナントへのアクセスと、脅威を検出するための SWC インスタンスが提供されます。SAL のユーザーは、これらの 2 つのポータルにアクセスして SAL が提供する結果を確認するために個別の CDO ライセンスまたは SWC ライセンスを必要としません。

SAL（SaaS） ライセンスオプションの詳細については、『*Cisco Security Analytics and Logging Ordering Guide*』（https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html）を参照してください。

SAL（SaaS） ライセンスは、Cisco Defense Orchestrator テナントを使用してファイアウォールログを表示する権利と、分析用の Stealthwatch Cloud（SWC）インスタンスを提供します。これらの製品のいずれかを使用するために個別のライセンスを保持する必要はありません。

SAL（SaaS） ライセンスを購入するには、シスコの認定セールス担当者に問い合わせるか、発注ガイド（前述のリンク） にアクセスして SAL-SUB で始まる PID を検索してください。

この製品に関する追加情報は次のとおりです。https://apps.cisco.com/Commerce/guest

ストレージ要件の計算とデータプランの購入

Cisco Cloud が ASA から毎日受け取るイベント数を反映したデータプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。

データストレージ要件を見積もるには、次の手順を実行します。

- （推奨）購入前に Cisco Security Analytics and Logging (SaaS) の無料トライアルに参加します。SAL（SaaS） ライセンス （4 ページ） を参照してください。
- https://ngfwpe.cisco.com/ftd-logging-estimator でロギングボリューム見積ツールを使用します。

データプランは、さまざまな日単位およびさまざまな年単位で利用できます。データプランの詳細については、『*Cisco Security Analytics and Logging Ordering Guide*』（https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html）を参照してください。

（注） SAL（SaaS） ライセンスとデータプランがある場合、その後は別のライセンスを取得するだけで、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで、別の SAL（SaaS） ライセンスを取得する必要はありません。

Syslog を使用した SAL（SaaS） でのイベントデータストレージの設定方法

	操作手順	詳細情報
ステップ	要件と前提条件を確認する	SAL（SaaS） 統合の要件と前提条件 （4 ページ）を参照してください。
ステップ	必要なライセンス、アカウント、およびデータストレージプランを取得する	シスコの認定営業担当者にお問い合わせください。
ステップ	多要素認証を使用して CDO アクセスをセットアップする	CDO へのサインインについては、CDO のオンラインヘルプに記載されている手順を参照してください。https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/0015_Signing_on_to_CDO
ステップ	VMWare仮想マシンでオンプレミスの Secure Device Connector（SDC）をセットアップする	このコンポーネントは、ASA デバイスがイベントを送信するコンポーネントである SEC のインストールを可能にするためにのみ必要です。 CDO のオンラインヘルプの説明に従って、次のいずれかを使用します。 • （推奨）CDO 提供の VM イメージを使用します。 • CDO 提供のイメージを使用せずに SDC を作成します。 **重要**手順の前提条件を省略しないでください。ただし、この統合には適用されないオンボーディングに関する情報は無視してください。
ステップ	作成した SDC 仮想マシンに Secure Event Connector（SEC）をインストールします。	これは、ASA デバイスがイベントを送信するコンポーネントです。 Secure Event Connector をインストールするには、CDO のオンラインヘルプを参照してください。 **重要**手順の前提条件を省略しないでください。ただし、この統合には適用されないオンボーディングに関する情報は無視してください。

	操作手順	詳細情報
ステップ	ASA に syslog イベントと NSEL イベントを SEC に送信させるように ASDM を設定します。	ASA デバイスからの syslog イベントの送信 （8 ページ）およびASA デバイスからの NetFlow Secure Event Logging（NSEL）データの送信 （12 ページ）
ステップ	イベントが正常に送信されていることを確認する	イベントの表示および操作 （15 ページ） を参照してください。
ステップ	（任意）CDO の一般設定を指定する	たとえば、シスコのサポートスタッフがデータを使用できないようにすることができます。 CDO のオンラインヘルプで、「一般設定」を参照してください。
ステップ	（任意）同僚がイベントを表示および操作するための CDO ユーザーアカウントを作成する	CDO のオンラインヘルプで、「新規 CDO ユーザーの作成」を参照してください。

CDO から SEC の IP およびポート番号を取得する方法

Cisco Cloud に接続するように ASA デバイスを設定するときには、SEC の IP とそのポート番号が必要です。CDO から SEC の詳細を取得するには、次の手順を実行します。

手順

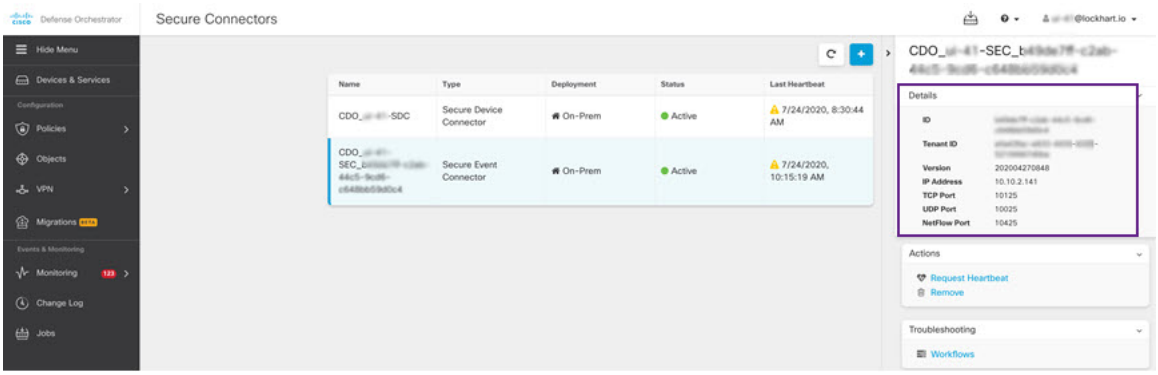
ステップ 1 CDO にサインインします。

ステップ 2 CDO ブラウザウィンドウの右上にあるユーザーメニューから、[セキュアコネクタ（Secure Connectors）] を選択します。

ステップ 3 [Secure Connectors] リストで、目的の SEC をクリックします。

ステップ 4 [Details] セクションで、設定されている IP アドレス、TCP、UDP、および NetFlow のポート番号を探します。

図 *1 : SEC* の *IP* およびポート番号の取得



ASA デバイスからの syslog イベントの送信

ASA のシステムログにより、ASA のモニタリングおよびトラブルシューティングに必要な情報が得られます。ASA イベントタイプのリストについては、こちらを参照してください。

ASA に、syslog イベントを SAL（SaaS） クラウドに送信させるには、ASA デバイスでロギングを設定する必要があります。

- ロギングの有効化
- SEC への出力先の設定

（注） EMBLEM ロギング形式とセキュアロギングは、この統合ではサポートされていません。

ASA CLI および ASDM でのロギング設定については、次のリンクを使用してください。

- ASA デバイスから syslog イベントを送信するための CLI コマンド （8 ページ）
- ASA デバイスから syslog イベントを送信するための ASDM 設定 （10 ページ）

ASA デバイスから syslog イベントを送信するための CLI コマンド

この手順では、セキュリティイベントの syslog メッセージを ASA デバイスから SAL に送信するための設定コマンドについて説明します。

始める前に

- 要件と前提条件のセクションを確認します。
- SAL（SaaS）でイベントデータストレージをセットアップします。
- ASA デバイスが SEC に到達できることを確認します。
- カスタム Linux VM に SDC をインストールした場合は、SEC が ASA syslog を受信することを確認します。
- CDO から SEC の IP アドレスとポート番号を取得します。

手順

ステップ 1 ロギングを有効にします。

logging enable

例：

```
ciscoasa(config)# logging enable
```

ステップ 2 syslog サーバー（SEC）に送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

例：

SEC に送信する syslog メッセージのシビラティ（重大度）の値（1 ー 7）または名前を指定できます。

```
ciscoasa(config)# logging trap errors
```

例：

また、SEC に送信する syslog メッセージを特定したカスタムメッセージリストを指定することもできます。

```
ciscoasa(config)# logging list specific_event_list message 106100
ciscoasa(config)# logging list specific_event_list message 302013-302018
ciscoasa(config)# logging trap specific_event_list
```

ステップ 3 Secure Event Connector（SEC）にメッセージを送信するように ASA を設定します。

logging host *interface_name syslog_ip* [**protocol**/*port*]

例：

```
ciscoasa(config)#  logging host management 209.165.201.3 6/10125

OR
ciscoasa(config)#  logging host management 209.165.201.3 17/10025
```

（注）
1. syslog_ip と port については、CDO から取得した SEC IP および対応するポート番号を指定します（手順については、「はじめる前に」を参照）。
2. TCP プロトコルを示すには *6* を指定し、UDP プロトコルを示すには *17* を指定します。

ステップ 4 （任意）syslog メッセージのタイムスタンプ形式を設定します。

logging timestamp {**legacy** | **rfc5424**}

例：

```
ciscoasa(config)# logging host tftp 1.1.1.1 tcp/1900 format ?

configure mode commands/options:
  analytics  Enable Analytics on syslog messages
  emblem     Enable EMBLEM format logging, available only for udp syslog messages
  timestamp  Enable logging timestamp on syslog messages
ciscoasa(config)# logging host tftp 1.1.1.1 tcp/1900 format timestamp ?

configure mode commands/options:
  legacy   Timestamp formatted as per legacy
  rfc5424  Timestamp formatted as per RFC5424
ciscoasa(config)# logging host tftp 1.1.1.1 tcp/1900 format timestamp rfc5424
```

RFC5424 で指定されているタイムスタンプの形式は yyyy-MM-THH:mm:ssZ です（文字 Z は UTC タイムゾーンを示す）。

（注） RFC5424 は、ASA 9.10(1) 以降でのみサポートされています。

ステップ 5 （任意）syslog メッセージをデバイス ID とともに表示するように ASA を設定します。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

例：

```
ciscoasa(config)# logging device-id context-name
```

EMBLEM ロギング形式は、この統合ではサポートされていません。そのため、syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

ASA デバイスから syslog イベントを送信するための ASDM 設定

この手順では、セキュリティイベントの ASA syslog メッセージを SAL（SaaS） に送信するための ASDM の設定について説明します。

始める前に

- 要件と前提条件のセクションを確認します。
- SAL（SaaS） でイベントデータストレージをセットアップします。
- ASA デバイスが SEC に到達できることを確認します。
- カスタム Linux VM に SDC をインストールした場合は、SEC が ASA syslog を受信することを確認します。
- CDO から SEC の IP アドレスとポート番号を取得します。

手順

ステップ 1 ASDM にログインします。

ステップ 2 ロギングを有効にします。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [ロギングのセットアップ（Logging Setup）]** をクリックします。

b) [Enable logging] チェックボックスをオンにして、ロギングをオンにします。

（注） この統合は EMBLEM 形式をサポートしていません。そのため、[EMBLEM で syslog を送信（Send syslogs in EMBLEM）] チェックボックスがオフになっていることを確認します。

ステップ 3 syslog サーバー（SEC）のロギングフィルタ設定を指定します。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [ロギングフィルタ（Logging Filters）]** を選択します。
b) テーブルから [syslog サーバー（Syslog Servers）] を選択し、[編集（Edit）] をクリックします。
c) [ロギングフィルタの編集（Edit Logging Filters）] ダイアログボックスで、次のいずれかのロギングフィルタ設定を選択します。

   重大度に基づいて syslog メッセージをフィルタ処理するには、[重大度によるフィルタ（Filter on severity）] をクリックし、重大度を選択します。

   （注） ASA は、指定されたレベルまでの重大度のシステムログメッセージを生成します。

   または

   メッセージ ID に基づいて syslog メッセージをフィルタ処理するには、[イベントリストの使用（Use event list）] をクリックします。必要な syslog メッセージ ID で作成されたイベントリストを選択するか、[新規（New）] をクリックして、syslog メッセージ ID または ID の範囲でリストを作成することができます。

d) 設定を保存します。

ステップ 4 SEC の IP アドレスとポートを使用して外部 syslog サーバーを設定します。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [syslog サーバー（Syslog Server）]** を選択します。
b) [追加（Add）] をクリックして、新しい Syslog サーバーを追加します。
c) [syslog サーバーの追加（Add Syslog Server）] ダイアログボックスで、次を指定します。
   - [インターフェイス（Interface）]：syslog サーバーとの通信に使用するインターフェイス。
   - [IP アドレス（IP Address）]：CDO から取得した SEC IP（手順については、「はじめる前に」を参照）。
   - [プロトコル（Protocol）]：TCP または UDP を選択します。
   - [ポート（Port）]：CDO から取得した、対応する SEC ポート番号（手順については、「はじめる前に」を参照）。

   （注） UDP を選択した場合は、[メッセージを Cisco EMBLEM 形式でロギング（Log messages in Cisco EMBLEM format）] チェックボックスを使用できます。この統合は EMBLEM 形式をサポートしていません。そのため、このチェックボックスがオフになっていることを確認します。

ステップ 5 [保存（Save）] をクリックして設定に変更を適用します。

ASA デバイスからの NetFlow Secure Event Logging（NSEL）データの送信

ASA は、NetFlow Secure Event Logging（NSEL）を使用して詳細な接続イベントデータをレポートします。サポートされる ASA NSEL イベントタイプのリストについては、こちらを参照してください。

この接続イベントデータ（双方向フロー統計を含む）に Stealthwatch Cloud 分析を適用できます。ASA からフローコレクタに NSEL イベントを送信させるには、ASA デバイスで NSEL を設定する必要があります。

- NetFlow コレクタを追加します。これは、ここでは Secure Event Connector（SEC）です。
- サービスポリシールールを設定します。
- NSEL イベントを介して送信される情報は、syslog 接続イベントの一部と重複しています。冗長な syslog メッセージが SEC に転送されないようにします。

ASA CLI および ASDM での NSEL 設定については、次のリンクを使用してください。

- ASA デバイスから NSEL データを送信するための CLI コマンド （12 ページ）
- ASA デバイスから NSEL データを送信するための ASDM 設定 （14 ページ）

ASA デバイスから NSEL データを送信するための CLI コマンド

この手順では、NSEL イベントを ASA デバイスから SAL（SaaS） に送信するための設定コマンドについて説明します。

始める前に

- 要件と前提条件のセクションを確認します。
- SAL（SaaS） でイベントデータストレージをセットアップします。
- ASA デバイスが SEC に到達できることを確認します。
- カスタム Linux VM に SDC をインストールした場合は、SEC が ASA イベントを受信することを確認します。
- CDO から SEC の IP アドレスとポート番号を取得します。

手順

ステップ 1 NetFlow パケットの送信先となる NetFlow コレクタを追加します。ここでは、Secure Event Connector（SEC）が NetFlow コレクタです。

flow-export destination *interface_name ipv4_address | host name udp-port*

例：

```
ciscoasa(config)# flow-export destination management 209.165.201.3 10425
```

（注） ipv4_address と udp-port については、CDO から取得した SEC の IP アドレスと UDP ポート番号を指定します（手順については、「はじめる前に」を参照）。

ステップ 2 NetFlow コレクタ（SEC）に NetFlow イベントを送信するようにポリシーを設定します。

a) NSEL イベントをエクスポートする必要があるトラフィックを識別するクラス マップを定義します。

class-map *flow_export_class*

例：

```
ciscoasa(config)# class-map global_class
```

b) 任意のトラフィックと照合します。

match any

例：

```
ciscoasa(config-cmap)# match any
```

c) 定義されたクラスに対する flow-export アクションを適用するポリシー マップを定義します。

policy-map *flow_export_policy*

例：

```
ciscoasa(config-cmap)# policy-map global_policy
```

d) flow-export アクションを適用するクラスを定義します。

class *flow_export_class*

例：

```
ciscoasa(config-pmap)# class global_class
```

e) flow-export アクションを設定します。

flow-export event-type *event-type* **destination** *flow_export_host1* [*flow_export_host2*]

例：

```
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.201.3
```

NetFlow コマンドの詳細については、『Cisco ASA NetFlow 実装ガイド』を参照してください。

ステップ 3 冗長な syslog メッセージを無効にします。

logging flow-export-syslogs disable

例：

```
ciscoasa(config)# logging flow-export-syslogs disable
```

ASA デバイスから NSEL データを送信するための ASDM 設定

この手順では、ASA の NetFlow Secure Event Logging（NSEL）イベントを SAL（SaaS） ソリューションに送信するための ASDM 設定について説明します。

始める前に

- 要件と前提条件のセクションを確認します。
- SAL（SaaS） でイベントデータストレージをセットアップします。
- ASA デバイスが SEC に到達できることを確認します。
- カスタム Linux VM に SDC をインストールした場合は、SEC が ASA イベントを受信することを確認します。
- CDO から SEC の IP アドレスとポート番号を取得します。

手順

ステップ 1 ASDM にログインします。

ステップ 2 NetFlow パケットの送信先となる NetFlow コレクタを追加します。ここでは、Secure Event Connector（SEC）が NetFlow コレクタです。

a) **[Configuration]** > **[Device Management]** > **[Logging]** > **[NetFlow]** を選択します。

b) [コレクタ（Collectors）] セクションで、[追加（Add）] をクリックしてコレクタを追加します。

c) [NetFlow コレクタの追加（Add NetFlow Collector）] ダイアログボックスで、次を指定します。

- [インターフェイス（Interface）]：NetFlow コレクタとの通信に使用するインターフェイスを指定します。
- [IP アドレスまたはホスト名（IP Address or Hostname）]：CDO から取得した SEC IP アドレス（手順については、「はじめる前に」を参照）。
- [UDP ポート（UDP Port）]：CDO から取得した SEC ポート番号（手順については、「はじめる前に」を参照）。

d) [OK] をクリックします。

ステップ 3 サービスポリシーを設定します。

a) **[設定（Configuration）]** > **[ファイアウォール（Firewall）]** > **[サービスポリシールール（Service Policy Rules）]** を選択します。

b) [追加（Add）] をクリックします。

c) [サービスポリシールールの追加ウィザード：サービスポリシー（Add Service Policy Rule Wizard - Service Policy）] で、[グローバル：すべてのインターフェイスに適用（Global - applies to all interfaces）] オプションボタンをクリックしてルールをグローバルポリシーに適用し、[次へ（Next）] をクリックします。

d) [サービスポリシールールの追加ウィザード：トラフィック分類基準（Add Service Policy Rule Wizard - Traffic Classification Criteria）] で、[すべてのトラフィック（Any traffic）] チェックボックスをオンにし、[次へ（Next）] をクリックします。

e) [サービスポリシールールの追加ウィザード：ルールアクション（Add Service Policy Rule Wizard - Rule Actions）] で、[NetFlow] タブをクリックし、[追加（Add）] をクリックします。

f) [フローイベントの追加（Add Flow Event）] ダイアログボックスで、ステップ 2 で追加したコレクタが [コレクタ（Collectors）] テーブルに一覧表示されます。[送信（Send）] 列でコレクタ（SEC）に対するチェックボックスをオンにして、[OK] をクリックします。

g) [終了（Finish）] をクリックします。

ステップ 4 冗長な syslog メッセージが SEC に転送されないようにします。

a) **[Configuration]** > **[Device Management]** > **[Logging]** > **[NetFlow]** を選択します。

b) [冗長な syslog メッセージの無効化（Disable redundant syslog messages）] オンにします。

c) [Apply] をクリックします。

ステップ 5 [保存（Save）] をクリックして設定に変更を適用します。

イベントの表示および操作

クラウドでイベントを表示および検索するには、次の手順を実行します。

手順

ステップ 1 ブラウザを使用して、イベントの送信先の地域 CDO クラウドに移動します。

- 北米：

  http://www.defenseorchestrator.com

- 欧州：

  http://www.defenseorchestrator.eu

ステップ 2 CDO にサインインします。

ステップ 3 ナビゲーションバーから、[モニタリング（Monitoring）] > [イベントロギング（Event Logging）] を選択します。

ステップ 4 [履歴（Historical）] タブを使用して履歴イベントデータを表示します。デフォルトでは、このタブがビューアに表示されます。

ステップ 5 ライブイベントを表示するには、[ライブ（Live）] タブをクリックします。

（注）　[イベントロギング（Event Logging）] ページは、次のようになっています。

- 詳細に解析された ASA syslog イベントはイタリック体で表示されます。
- NetFlow イベントを表示するには、[フィルタ（Filters）] ペインの [ASA イベント（ASA Events）] で [NetFlow] チェックボックスをオンにします。NetFlow イベントは、イベントタイプ値（1、2、3、および 5）で識別できます。
- [フィルタ（Filters）] ペインの下部にある [NetFlow イベントを含める（Include NetFlow Events）]チェックボックスは、デフォルトでオンになっています。イベントをフィルタ処理して [ファイアウォール拒否（Firewall Denied）] および [ファイアウォールトラフィック（Firewall Traffic）] を表示すると、NetFlow イベントも syslog イベントとともに表示されます。

このページで実行できることの詳細については、CDO のオンラインヘルプでイベント表示の手順を参照してください。

次のタスク

Logging Analytics and Detection ライセンスまたは **Total Network Analytics and Detection** ライセンスがある場合は、CDO のオンラインヘルプで手順を参照して Stealthwatch Cloud ポータルを相互起動してください。

FAQ

ASA デバイスを CDO にオンボードする必要はありますか。

いいえ。デバイスを CDO にオンボードしないでください。

SAL（SaaS）でも CDO と Stealthwatch Cloud のライセンスが必要ですか。

いいえ。SAL（SaaS）は、イベントを表示するために Cisco Defense Orchestrator（CDO）を使用し、動作を検出するために Stealthwatch Cloud（SWC）を使用する権利を提供します。これら 2 つの製品のライセンスを個別に保持する必要はありません。ただし、SWC の診断および分析の機能を使用するには、適切なライセンスを取得する必要があります。

ASA をアップグレードする場合は、データプランもアップグレードする必要がありますか。

いいえ。データプランは、Cisco Cloud が ASA から毎日受け取るイベント数に基づいています。デバイスのバージョンに関係なく、データプランを変更できます。「ストレージ要件の計算とデータプランの購入 （5 ページ）」を参照してください。

CDO イベントビューアにイベントが表示されません。何をすればよいですか。

1. SEC で実行されているサービスと、そのサービスと Cisco Cloud との接続の基本的なヘルスチェックを実行します。ヘルスチェックを実行するには、sdc ユーザーとして SDC VM にいる必要があります。詳細については、Cisco Defense Orchestrator のガイドを参照してください。

2. ASA が正しい SEC の IP アドレスと TCP/UDP ポートで設定されていることを確認します。

問題が解決しない場合は、Cisco Defense Orchestrator サポートにお問い合わせください。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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/

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。