外部ツールを使用したイベントの分析

Cisco Cloud イベント設定

ファイアウォールイベントをクラウドに送信すると、外部ツールを使用してファイアウォールインシデントを調査できます。デバイスは、Security Services Exchange（SSE）にファイアウォールイベントを送信します。ここから、さまざまなクラウドサービスに転送して、可視性を統合し、脅威調査を強化することができます。

デバイスが Cisco Security Cloud にファイアウォールイベントを送信できるようにするには、Firewall Management Center をスマートライセンスに登録するか（[システム（System）]（⚙）> **[スマートライセンス（Smart License）]**）、Cisco Security Cloud統合を有効にする必要があります。Cisco Security Cloud 統合により、Firewall Management Center が Security Cloud Control アカウントに関連付けられ、Cisco Secure Firewall 展開が Cisco Cloud テナントに導入準備され、シスコの統合セキュリティ クラウド サービスに接続できるようになります。

Firewall Management CenterとCisco Security Cloudの統合の詳細については、Cisco Security Cloud 統合の有効化を参照してください。

Security Services Exchange イベント統合

Security Services Exchange には、 Firewall Management Centerからのイベントの完全なリストは表示されません。代わりに、イベントを関連付けて統合し、一意のイベントだけを表示します。このアプローチにより、イベントの冗長性が低減され、明確性が向上します。この統合に使用される現在の分類パラメータの詳細は次のとおりです。

- 侵入イベントの重複を特定するために、イニシエータ IP、イニシエータ IP、SID、および GID の各要素が考慮されます。
- 接続イベントとセキュリティ関連の接続イベントの重複を特定するため、[イニシエータ IP（Initiator IP）]、[イニシエータ IP（Initiator IP）]、[セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] の各要素が考慮されます。
- ファイルイベントおよびマルウェアイベントの重複を特定する場合、Event Second 以外のすべての要素が考慮されます。

Cisco Security Cloud にイベント送信できるようにする

管理対象 Firewall Threat Defense デバイスにイベントを直接 Cisco Security Cloud に送信させるように Firewall Management Center を設定します。このページで設定するクラウド地域とイベントタイプは、適用可能で有効になっている場合、複数の統合に使用できます。

始める前に

- ファイアウォールイベントの送信に使用するシスコ地域クラウドを決定します。地域クラウドを選択する際は、次の点に注意してください。
  - 選択した地域クラウドは、Cisco Support Diagnostics および Cisco Support Network 機能にも使用されます。この設定は、シスコのセキュリティ分析とロギング（SaaS）を使用する Secure Network Analytics クラウドのクラウド地域も管理します。
  - 複数の地域クラウドのデータをマージまたは集約することはできません。複数の地域からデータを集約するには、すべての地域のデバイスが同じ地域クラウドにデータを送信する必要があります。
- Management Center をスマートライセンスに登録（[システム（System）]（⚙）>**[スマートライセンス（Smart License）]**）しているか、Cisco Security Cloud 統合を有効にして、デバイスがファイアウォールイベントを Cisco Cloud に送信できるようになっていることを確認します。

（注） バージョン 7.6 より前の SecureX サブスクリプションを使用してすでに Cisco Security Cloud にイベントを送信していた場合は、Cisco XDR などの Cisco Security Cloud サービスに引き続きイベントを送信できます。ただし、Security Cloud Control アカウントを使用してクラウドテナントに Management Center を登録する場合、Security Cloud Control アカウントには、Cisco XDR などの Cisco Security Cloud サービスにイベントを転送するためのセキュリティ分析とロギング ライセンスが必要です。

- Firewall Management Center で次の手順を実行します。

- [システム（System）] > [設定（Configuration）] ページに移動し、クラウドの [デバイス（Devices）] リストで明確に識別される一意の名前を Firewall Management Center に付けます。
- Firewall Threat Defense デバイスを Firewall Management Center に追加し、それらにライセンスを割り当て、システムが正常に動作していることを確認します必要なポリシーが作成され、生成されたイベントが Firewall Management Center UI の [分析（Analysis）] メニューに想定どおりに表示されているかを確認します。

- Cisco Security Cloud Sign On ログイン情報があり、アカウントが作成された地域クラウドにサインインできることを確認します。

  地域クラウドURL とサポートされているデバイスバージョンの詳細については、「Regional Clouds」[英語] を参照してください。
- スマートアカウントまたは Security Cloud Control テナントを SSE アカウントにリンクしていることを確認します。
- 現在 syslog を使用してクラウドにイベントを送信している場合は、重複を避けるために無効にします。

手順

ステップ 1 ファイアウォールイベントの送信に使用する地域クラウドを決定します。地域クラウドの選択の詳細については、『Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide』[英語] を参照してください。

（注）
Cisco Security Cloud の統合が有効になっていて、選択した地域クラウドに Firewall Management Center が登録されている場合、地域クラウドを変更すると Cisco Security Cloud の統合が無効になります。地域クラウドを変更した後、Cisco Security Cloud の統合を再度有効にすることができます。

ステップ 2 Firewall Management Center で、**[統合（Integration）]** > **[Cisco Security Cloud]** をクリックします。

ステップ 3 [現在のリージョン（Current Region）] ドロップダウンリストから地域クラウドを選択します。

ステップ 4 [クラウドにイベントを送信（Send events to the cloud）] チェックボックスをオンにして、クラウドイベント設定を有効にします。

ステップ 5 クラウドに送信するイベントのタイプを選択します。

（注）
次の表に示すように、クラウドに送信するイベントを複数の統合に使用できます。

統合	サポートされるイベントのオプション	注意
Cisco Security Analytics and Logging (SaaS)	すべて（All）	優先順位の高い接続イベントには、次のイベントが含まれます。 • セキュリティ関連の接続イベント • ファイルおよびマルウェア イベントに関連する接続イベント • 侵入イベントに関連する接続イベント
Cisco Extended Detection and Response（Cisco XDR）	お使いのバージョンに応じて、以下が含まれます。 • セキュリティ関連の接続イベント。 • 侵入イベント。 • ファイルイベントおよびマルウェアイベント。	すべての接続イベントを送信する場合でも、Cisco XDR ではセキュリティ関連の接続イベントのみがサポートされます。 （注） Cisco XDR は別個にライセンス供与される製品です。Cisco Secure Firewall 製品に必要なライセンス以外に、追加のサブスクリプションが必要です。詳細については、「Cisco XDR Licenses」を参照してください。

（注）
- **侵入イベント**を有効にすると、Firewall Threat Defense デバイスは、イベントと影響フラグを送信します。
- [ファイルおよびマルウェアイベント（File and Malware Events）] を有効にすると、Firewall Threat Defense デバイスから送信されるイベントに加えて、レトロスペクティブイベントが Firewall Management Center から送信されます。

ステップ 6 [保存（Save）] をクリックします。

Cisco XDR を使用したイベントの分析

Cisco Extended Detection and Response （Cisco XDR） は、複数のテレメトリソースの検出を関連付けることで可視性を統合し、セキュリティチームが最も高度な脅威を検出、優先順位付けして対応できるようにするクラウドベースのソリューションです。Firewall Threat Defense を Cisco XDR と統合することにより、シスコの統合型セキュリティポートフォリオをお客様ファイアウォール展開とつなぎ、可視性の統合、自動化、ネットワーク全体のセキュリティの強化を実現する一貫したエクスペリエンスを提供します。

Cisco XDR の詳細については、Cisco XDR ヘルプ センターにアクセスしてください。

重要

- Cisco XDR は別個にライセンス供与される製品です。Cisco Secure Firewall 製品に必要なライセンス以外に、追加のサブスクリプションが必要です。詳細については、「Cisco XDR Licenses」を参照してください。
- バージョン 7.6 より前の SecureX サブスクリプションを使用してすでに Cisco Security Cloud にイベントを送信していた場合は、Cisco XDR に引き続きイベントを送信できます。ただし、Security Cloud Control アカウントを使用してクラウドテナントに Firewall Management Center を登録し、ファイアウォールイベントを Cisco XDR に送信する場合、Security Cloud Control アカウントには、Cisco XDR にイベントを転送するための セキュリティ分析とロギング ライセンスが必要です。

Firewall Threat Defense と Cisco XDR を統合するには、Cisco セキュア ファイアウォール脅威防御と Cisco XDR 統合ガイドを参照してください。

（注） 2024 年 7 月 31 日の段階で Cisco SecureX は廃止され、使用できなくなりました。Cisco SecureX をユーザー向けにプロビジョニングすることはできず、Cisco Secure Firewall 製品を購入しても Cisco SecureX へのアクセスは提供されません。さらに、既存のすべての Cisco SecureX 環境が無効になり、すべての機能が使用できなくなります。Firefox を使用している場合は、Cisco SecureX Ribbon ブラウザ拡張機能を削除してください。詳細については、よくある質問（FAQ）を参照してください。

Cisco XDR 自動化を使用した脅威の分析と対応

この設定を有効にすると、Cisco Extended Detection and Response（Cisco XDR）ユーザーが作成した自動ワークフローが Firewall Management Center リソースと連携できるようになります。

Cisco XDR 自動化は、自動ワークフローを構築するためのノーコード ローコード アプローチを提供します。ドラッグアンドドロップインターフェイスで独自のワークフローを設計でき、さまざまなスケジュールやイベントに応じて実行するように設定できます。Cisco XDR 自動化により、関連するすべてのコントロールポイントで自動化とガイド付きの推奨対応方法を使用して脅威を修復できます。

（注） Cisco XDR は別個にライセンス供与される製品です。Cisco Secure Firewall 製品のライセンス以外に、追加のサブスクリプションが必要です。詳細については、「Cisco XDR Licenses」を参照してください。

Cisco XDR 自動化機能の詳細については、Cisco XDR のドキュメントを参照してください。

始める前に

Cisco Security Cloud を有効にし、Management Center をクラウドに登録します。Cisco Security Cloud 統合の有効化 を参照してください。

手順

ステップ 1 **[統合（Integration）] > [Cisco Security Cloud]** をクリックします。

ステップ 2 [Cisco XDR自動化の有効化（Enable Cisco XDR Automation）] チェックボックスをオンにします。

ステップ 3 Cisco XDR 自動化ワークフローに割り当てる Firewall Management Center ユーザーロールを選択します。

[アクセス管理者（Access Admin）] ロールがデフォルトとして設定され、[ポリシー（Policies）] メニューのアクセス コントロール ポリシーおよび関連機能へのアクセスが許可されます。

ステップ 4 [保存（Save）] をクリックします。

Web ベースのリソースを使用したイベントの調査

Secure Firewall Management Center 外部の Web ベースのリソースにおける潜在的な脅威についての情報をすばやく検索するには、コンテキスト クロス起動 機能を使用します。例：

- Cisco または既知の疑わしい脅威に関する情報を公開するサードパーティ製クラウドホステッド サービスの疑わしい送信元 IP アドレスを検索する、または
- 組織の履歴ログで特定の脅威に関する過去のインスタンスを検索する（組織がセキュリティ情報とイベント管理（SIEM）アプリケーションでそのデータを格納している場合）。
- 組織で Cisco Secure Endpoint を導入している場合は、ファイルトラジェクトリ情報などの特定のファイルに関する情報を検索します。

イベントを調査する際は、Secure Firewall Management Center のイベント ビューアまたはダッシュボードのイベントから直接、外部リソースの関連情報をクリックできます。これにより、その IP アドレス、ポート、プロトコル、ドメイン、または SHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

たとえば、[上位攻撃者（Top Attackers）] ダッシュボード ウィジェットを表示し、記載されている送信元 IP アドレスのいずれかに関する詳細情報を検索すると仮定します。この IP アドレスに関して、Talos がどのような情報を公開しているか確認したいので、「Talos IP」リソースを選択します。Talos Web サイトが開き、この特定の IP アドレスに関する情報が書かれたページが表示されます。

一般的に使用されているシスコやサードパーティ製の脅威インテリジェンス サービスへの一連の事前定義されたリンクから選択し、その他の Web ベースのインターフェイスおよび Web イ

ンターフェイスを持つ SIEM または他の製品へのカスタム リンクを追加できます。一部のリソースでは、アカウントまたは製品の購入が必要になる場合があります。

コンテキスト クロス起動のリソースの管理について

[分析（Analysis）]>[詳細（Advanced）]>[コンテキスト クロス起動（Contextual Cross-Launch）] ページを使用して外部の Web ベースのリソースを管理します。

例外：Secure Network Analytics の相互起動リンクの設定 （10 ページ）の手順に従って、Secure Network Analytics アプライアンスへのクロス起動リンクを管理します。

シスコが提供している事前定義のリソースにはシスコのロゴが付いています。残りのリンクはサードパーティのリソースです。

必要がないリソースは無効にするか、または削除できます。あるいは、たとえば名前の前に小文字の「z」を追加するなどして名前を変更し、そのリソースをリストの下部に分類することができます。クロス起動リソースを無効にすると、すべてのユーザーに対して無効になります。削除されたリソースは、元に戻すことはできませんが、再作成できます。

リソースを追加するには、コンテキスト クロス起動のリソースの追加 （7 ページ）を参照してください。

カスタム コンテキスト クロス起動のリソースの要件

カスタム コンテキスト クロス起動 リソースを追加する場合は、次の点に留意します。

- リソースは Web ブラウザを介してアクセスできる必要があります。
- http プロトコルと https プロトコルのみがサポートされています。
- GET 要求のみがサポートされています。POST 要求はサポートされていません。
- URL の変数のエンコーディングはサポートされていません。IPv6 アドレスをエンコードするにはコロンで区切る必要がある場合がありますが、ほとんどのサービスでこのエンコーディングは必要ありません。
- 事前に定義されたリソースを含めて、最大 100 のリソースを設定できます。
- 相互起動を作成するには管理者またはセキュリティ アナリスト（Security Analyst）のユーザーである必要がありますが、読み取り専用のセキュリティ アナリスト（Security Analyst）でも使用できます。

コンテキスト クロス起動のリソースの追加

脅威インテリジェンス サービスやセキュリティ情報とイベント管理（SIEM）の ツールなどのコンテキスト クロス起動 リソースを追加できです。

マルチドメイン展開環境では、親ドメインのリソースを表示および使用できますが、現在のドメインで実行できるのはリソースの作成と編集のみです。すべてのドメインのリソースの合計数は 100 に制限されています。

始める前に

- Secure Network Analytics アプライアンスにリンクを追加する場合は、必要なリンクがすでに存在するかどうかを確認してください。ほとんどのリンクは、セキュリティ分析とロギング（オンプレミス） の構成時に作成されます。
- カスタム コンテキスト クロス起動のリソースの要件 （7 ページ）を参照してください。
- リソースに必要な場合は、アクセスに必要なアカウントとクレデンシャルにリンクするか、作成するか、または取得します。必要に応じて、アクセスが必要な各ユーザーにクレデンシャルを割り当てて配布します。
- リンク先のリソースのクエリ リンクのシンタックスを特定します。

  ブラウザ経由でリソースにアクセスし、必要に応じてそのリソースのドキュメントを使用して、たとえば IP アドレスなど、検索するクエリ リンクの特定のタイプの情報の検索に必要なクエリ リンクを作成します。

  クエリを実行して、結果の URL をブラウザのロケーション バーからコピーします。

  たとえば、クエリ URL **`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`** が表示される場合があります。

手順

ステップ 1 **[分析（Analysis）] > [詳細（Advanced）] > [コンテキスト クロス起動（Contextual Cross-Launch）]** を選択します。

ステップ 2 [新しい相互起動（New Cross-launch）] をクリックします。

表示されたフォームのアスタリスクの付いたすべてのフィールドに値が必要です。

ステップ 3 一意のリソース名を入力します。

ステップ 4 作業中の URL の文字列をリソースから [URL テンプレート（URL Template）] フィールドに貼り付けます。

ステップ 5 クエリ文字列内の特定のデータ（IP アドレスなど）を適切な変数で置き換えます。変数を挿入するには、カーソルを置いて変数（[ip] など）を 1 回クリックします。

上記の「開始する前に」の項の例では、URL は **`https://www.talosintelligence.com/reputation_center/lookup?search= {ip}`** になります。コンテキスト クロス起動 リンクを使用すると、URL 内の {ip} 変数は、イベント ビューアまたはダッシュボードでユーザーが右クリックする IP アドレスに置き換わります。

各変数の説明については、変数の上にカーソルを置きます。

1 つのツールまたはサービスに複数の コンテキスト クロス起動 リンクを作成するには、それぞれに異なる変数を使用します。

ステップ 6 [サンプルデータを使用したテスト（test with example data）]（  ）をクリックして、サンプルデータでリンクをテストします。

ステップ 7 問題を修正します。

ステップ 8 [保存（Save）] をクリックします。

コンテキスト クロス起動を使用したイベントの調査

始める前に

アクセスするリソースにクレデンシャルが必要な場合は、それらのクレデンシャルがあることを確認します。

手順

ステップ 1 Secure Firewall Management Center でイベントが表示される次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベント ビューア ページ（イベントのテーブルが含まれている [分析（Analysis）] メニューにあるオプション）

ステップ 2 対象のイベントを右クリックして、使用する コンテキスト クロス起動 のリソースを選択します。

必要に応じて、コンテキストメニューを下にスクロールして使用可能なすべてのオプションを確認します。

右クリックしたデータ タイプによって表示されるオプションが異なります。たとえば、IP アドレスを右クリックした場合は、IP アドレスに関連する コンテキスト クロス起動 のオプションのみが表示されます。

たとえば、侵入イベントの送信元 IP アドレスについて Cisco Talos から脅威インテリジェンスを取得するには、[Talos SrcIP] または [Talos IP] を選択します。

リソースに複数の変数が含まれている場合、そのリソースを選択するオプションは、含まれている各変数に可能な 1 つの値を持つイベントにのみ使用できます。

別のブラウザ ウィンドウに コンテキスト クロス起動 のリソースが開きます。

クエリを実行するデータの量、リソースの速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

ステップ 3 必要に応じて、リソースにサインインします。

Secure Network Analytics の相互起動リンクの設定

Firewall Threat Defense のイベントデータから Secure Network Analytics アプライアンスの関連データに相互起動できます。Secure Network Analytics 製品の詳細については、Cisco Security Analytics and Logging の製品ページを参照してください。

コンテキストに応じた相互起動に関する一般的な情報については、コンテキストクロス起動を使用したイベントの調査 （9 ページ）を参照してください。

Secure Network Analytics アプライアンスへの一連の相互起動リンクを設定するには、この手順を使用します。

（注）

- 相互起動リンクを後で変更する場合は、この手順に戻ります。コンテキストに応じた相互起動リストページで直接変更することはできません。
- コンテキストクロス起動のリソースの追加 （7ページ）の手順を使用して、Secure Network Analytics アプライアンスに相互起動する追加のリンクを手動で作成できますが、それらのリンクは自動作成されたリソースからは独立しているため、手動で管理する必要があります。

始める前に

- 展開済みで実行中の Secure Network Analytics アプライアンスが必要です。
- 現在、イベントの直接送信をサポートしているデバイスのバージョンから Secure Network Analytics に syslog を使用してイベントを送信している場合、それらのデバイスの syslog を無効にして（または syslog の設定を含めないアクセス コントロール ポリシーをそれらのデバイスに割り当てて）リモートボリュームでイベントが重複しないようにします。
- 次のものが必要です。
  - マネージャのホスト名または IP アドレス。
  - 管理者権限を持つ Secure Network Analytics アプライアンスのアカウントのログイン情報。

セキュリティ分析とロギング（オンプレミス） を使用して Firewall Threat Defense データを Secure Network Analytics アプライアンスに送信する場合は、Secure Network Analytics アプライアンスでのリモートデータストレージを参照してください。

手順

ステップ 1 **[統合（Integration）]** > **[セキュリティ分析とロギング（Security Analytics & Logging）]** を選択します。

ステップ 2 Secure Network Analytics の展開には次の 2 つのオプションがあります。

- [Managerのみ（Manager Only）]：スタンドアロンの Manager を展開してイベントを受信および保存し、保存したイベントを確認およびクエリできます。
- [データストア（Data Store）]：Cisco Secure Network Analytics フローコレクタを展開してイベントを受信し、Secure Network Analytics データストアでイベントを保存し、Manager で保存したイベントを確認およびクエリできます。

展開オプションを選択し、[開始（Start）] をクリックします。

ステップ 3 ウィザードを完了します。詳細については、Cisco Security Analytics and Logging ファイアウォールイベント統合ガイド [英語] の「Firewall Management Center Configuration」を参照してください。

ステップ 4 **[分析（Analysis）]** > **[詳細（Advanced）]** > **[状況に応じた相互起動（Contextual Cross-launch）]** を選択して、新しい相互起動リンクを確認します。

変更する場合は、この手順に戻ります。コンテキストに応じた相互起動リストページで直接変更することはできません。

次のタスク

イベントから Secure Network Analytics イベントビューアに相互起動するには、Secure Network Analytics のログイン情報を使用します。

Firewall Management Center イベントビューアまたはダッシュボードのイベントから相互起動するには、関連するイベントのテーブルセルを右クリックし、適切なオプションを選択します。

処理するデータの量、Secure Network Analytics Manager の速度と需要などによって、クエリの処理に時間がかかる場合があります。

セキュリティイベントの syslog メッセージの送信について

接続、セキュリティインテリジェンス、侵入、およびファイルとマルウェアのイベントに関連するデータは、syslog を介してセキュリティ情報およびイベント管理（SIEM）ツールまたは、外部のイベントストレージおよび管理ソリューションに送信できます。

これらのイベントを Snort® イベントと呼ぶこともあります。

（注） バージョン 7.2.1 では、ルートルックアップを使用して syslog トラフィックを転送できたため、ロギングホスト設定で指定されたインターフェイスに関係なく、トラフィックを転送できました。ただし、バージョン 7.2.5.1 以降では、7.2.1 で導入された変更が削除されたため、

ロギングホスト設定で指定された設定がルートルックアップよりも優先され、syslog トラフィックは指定されたインターフェイスから転送されます。

syslog にセキュリティイベントデータを送信するためのシステムの設定について

セキュリティ イベントを syslog に送信するようにシステムを設定するには、次を知っておく必要があります。

- セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （12 ページ）
- セキュリティ イベントの syslog の設定場所 （18 ページ）
- Cisco Secure Firewall Management Center デバイス構成ガイドのセキュリティ イベントの *syslog* メッセージに適用する *FTD* プラットフォームの設定
- ポリシーで syslog の設定を変更した場合、それらの変更を有効にするには展開する必要があります。

セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス

デバイスとバージョン	設定の場所
すべて（All）	syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

デバイスとバージョン	設定の場所
Secure Firewall Threat Defense	1. Firewall Threat Defense プラットフォーム設定（[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]>[Threat Defense設定（Threat Defense Settings）]>[Syslog]）を設定します。 1. **[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]** をクリックします。 2. Threat Defense 設定ポリシーを編集します。 3. 左側のナビゲーションペインで、[Syslog] をクリック。 Cisco Secure Firewall Management Center デバイス構成ガイド の「セキュリティイベントの *syslog* メッセージに適用する *Threat Defense* プラットフォームの設定」も参照してください。 2. アクセス コントロール ポリシーの [ロギング（Logging）] タブで、Firewall Threat Defense プラットフォーム設定の使用を選択します。 3. （侵入イベントの場合）アクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用するように侵入ポリシーを設定します。（これはデフォルトです）。 これらの設定の上書きは推奨していません。 最低限必要な詳細情報については、Firewall Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信（14 ページ）を参照してください。
その他のすべてのデバイス	1. アラート応答を作成します。 2. アラート応答を使用するには、アクセス コントロール ポリシーの [ロギング（Logging）] を設定します。 3. （侵入イベントの場合）侵入ポリシーで syslog 設定を構成します。 詳細については、従来型デバイスからのセキュリティイベント syslog メッセージの送信 （17 ページ）を参照してください。

Firewall Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信

この手順では、Firewall Threat Defense デバイスからセキュリティイベント（接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアイベント）の syslog メッセージを送信するためのベストプラクティス設定について説明します。

（注） 多くの Firewall Threat Defense syslog 設定は、セキュリティイベントには適していません。この手順で説明するオプションのみを設定してください。

始める前に

- Secure Firewall Management Center で、セキュリティイベントを生成するようにポリシーを設定するとともに、予期されるイベントが [分析（Analysis）] メニューの該当するテーブルに表示されることを確認します。
- syslog サーバーの IP アドレス、ポート、およびプロトコル（UDP または TCP）を収集します。
- デバイスが syslog サーバーに到達できることを確認します。
- syslog サーバーがリモートメッセージを受け入れられることを確認します。
- 接続ロギングに関する重要な情報については、接続ロギングの関連する章を参照してください。

手順

ステップ 1 Firewall Threat Defense デバイスの syslog 設定を指定します。

a) [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] をクリックします。
b) Firewall Threat Defense デバイスに関連付けられているプラットフォーム設定ポリシーを**編集**します。
c) 左側のナビゲーションペインで、[Syslog] をクリック。
d) [syslogサーバー（Syslog Servers）] をクリックし、[追加（Add）] (＋) をクリックして、サーバー、プロトコル、インターフェイス、および関連情報を入力します。

このページのオプションについて疑問がある場合は、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

e) [syslog 設定（Syslog Settings）] をクリックし、次の設定を行います。

- syslogメッセージのタイムスタンプを有効化（Enable timestamp on syslog messages）
- **タイムスタンプ形式**
- syslogデバイスIDを有効化（Enable syslog device ID）

f) [ロギングのセットアップ（Logging Setup）] をクリックします。
g) [Basic Logging Settings（基本ロギング設定）] で、EMBLEM 形式で syslog を送信するかどうかを選択します。
h) [保存（Save）] をクリックして設定を保存します。

ステップ 2 アクセス コントロール ポリシーの一般的なログ設定（ファイルおよびマルウェアロギングを含む）を指定します。

a) [ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックします。
b) 該当するアクセス コントロール ポリシーを編集します。
c) **[詳細（More）]** > **[ロギング（Logging）]** をクリックします。
d) Firewall Threat Defense 6.3 以降：[デバイスに展開したFTDプラットフォーム設定のsyslog設定を使用する（Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）] をオンにします。
e) （任意）**syslog の重大度**を選択します。
f) ファイルおよびマルウェアイベントを送信する場合は、[ファイル/マルウェアイベントのsyslogメッセージを送信する（Send Syslog messages for File and Malware events）] をオンにします。
g) [**保存（Save**）] をクリックします。

ステップ 3 アクセス コントロール ポリシーのセキュリティ インテリジェンス イベントのロギングを有効にします。

a) 同じアクセス コントロール ポリシーで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。
b) 次の各場所で、**ロギング**（ ） をクリックし、接続の開始および終了と [syslog サーバー（Syslog Server）] を有効にします。
   - [DNS ポリシー（DNS Policy）] の横。
   - [ブロックリスト（Block List）]ボックスの、[ネットワーク（Networks）] と [URL（URLs）]。
c) [**保存（Save**）] をクリックします。

ステップ 4 アクセス コントロール ポリシーの各ルールの syslog ロギングを有効にします。

a) 同じアクセス コントロール ポリシーで、**[アクセスコントロール（Access Control）]** > **[ルールの追加（Add Rule）]** をクリックします。
b) 編集するルールを選択します。
c) ルールの [ロギング（Logging）] タブをクリックします。
d) 接続の開始時または終了時あるいはその両方をログに記録するかどうかを選択します。

   （接続ロギングでは大量のデータが生成されます。開始時と終了時の両方のロギングでは、生成されるデータの量がほぼ倍になります。すべての接続を開始時と終了時の両方でログに記録できるわけではありません）

e) ファイルイベントをログに記録する場合は、[ファイルのロギング（Log Files）] を選択します。

f) [syslog サーバー（Syslog Server）] を有効にします。
g) ルールが [アクセスコントロールログでデフォルトの syslog 設定を使用する（Using default syslog configuration in Access Control Logging）] であることを確認します。
h) [確認（Confirm）] をクリックします。
i) ポリシーの各ルールに対して手順を繰り返します。

ステップ 5 侵入イベントを送信する場合は、次の手順を実行します。

a) アクセス コントロール ポリシーに関連付けられている侵入ポリシーに移動します。
b) 侵入ポリシーで、[詳細設定（Advanced Settings）] > [Syslog アラート（Syslog Alerting）] > [有効（Enabled）] をクリックします。
c) 必要に応じて、[編集（Edit）] をクリックします。
d) オプションを入力します。

オプション	値
ロギングホスト	他の syslog メッセージを送信する syslog サーバーとは異なるサーバーに侵入イベントの syslog メッセージを送信するのでなければ、空白のままにします（前の手順で指定した設定が使用される）。
ファシリティ	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 説明については、Syslog アラート ファシリティを参照してください。
重大度	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 説明については、syslog 重大度レベルを参照してください。

e) [戻る（Back）] をクリックします。
f) 左側にあるナビゲーションウィンドウの [ポリシー情報（Policy Information）] をクリックします。
g) [変更を確定（Commit Changes）] をクリックします。

次のタスク

- （任意）個別のポリシーおよびルールに異なるロギング設定を指定します。

  にある該当する表の行を参照してください。

  これらの設定には、Syslog アラート応答の作成の説明に従って設定される syslog アラート応答が必要です。この手順で指定したプラットフォーム設定は使用されません。

- 従来型デバイスのセキュリティイベント syslog ロギングを設定するには、従来型デバイスからのセキュリティイベント syslog メッセージの送信 （17 ページ）を参照してください。

- 変更が完了したら、変更を管理対象デバイスに展開します。

従来型デバイスからのセキュリティイベント syslog メッセージの送信

始める前に

- セキュリティイベントを生成するポリシーを設定します。
- デバイスが syslog サーバーに到達できることを確認します。
- syslog サーバーがリモートメッセージを受け入れられることを確認します。
- 接続ロギングに関する重要な情報については、接続ロギングの章を参照してください。

手順

ステップ 1 従来型デバイスのアラート応答を設定します。

Syslog アラート応答の作成 を参照してください。

ステップ 2 アクセス コントロール ポリシーで syslog 設定を指定します。

a) [ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックします。
b) 該当するアクセス コントロール ポリシーを編集します。
c) [ロギング（Logging）] をクリックします。
d) [特定の syslog アラートを使用して送信する（Send using specific syslog alert）] をオンにします。
e) 上記で作成した **syslog アラート**を選択します。
f) [**保存（Save**）] をクリックします。

ステップ 3 ファイルイベントとマルウェアイベントを送信する場合は、次の手順を実行します。

a) [ファイル/マルウェアイベントの syslog メッセージを送信する（Send Syslog messages for File and Malware events）] をオンにします。
b) [**保存（Save**）] をクリックします。

ステップ 4 侵入イベントを送信する場合は、次の手順を実行します。

a) アクセス コントロール ポリシーに関連付けられている侵入ポリシーに移動します。
b) 侵入ポリシーで、[詳細設定（Advanced Settings）] > [Syslog アラート（Syslog Alerting）] > [有効（Enabled）] をクリックします。
c) 必要に応じて、[編集（Edit）] をクリックします。
d) オプションを入力します。

オプション	値
ロギングホスト	他の syslog メッセージを送信する syslog サーバーとは異なるサーバーに侵入イベントの syslog メッセージを送信するのでなければ、空白のままにします（前の手順で指定した設定が使用される）。
ファシリティ	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 Syslog アラート ファシリティ を参照してください。
重大度	この設定は、このページでロギングホストを指定した場合にのみ適用されます。 syslog 重大度レベル を参照してください。

e) [戻る（Back）] をクリックします。
f) 左側にあるナビゲーションウィンドウの [ポリシー情報（Policy Information）] をクリックします。
g) [変更を確定（Commit Changes）] をクリックします。

次のタスク

- （オプション）アクセス コントロール ルールごとに異なるロギング設定を指定します。接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス） （19 ページ） の該当するテーブル行を参照してください。これらの設定には、Syslog アラート応答の作成の説明に従って設定される syslog アラート応答が必要です。前の手順で指定した設定は使用されません。
- FTD デバイスのセキュリティイベント syslog ロギングを設定するには、Firewall Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信 （14 ページ） を参照してください。

セキュリティ イベントの syslog の設定場所

- 接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス） （19 ページ）。
- 侵入イベントの syslog の設定場所（FTD デバイス） （21 ページ）。
- 侵入イベントの syslog の設定場所（FTD 以外のデバイス） （22 ページ）。
- ファイルとマルウェア イベントの syslog の設定場所 （22 ページ）。

接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス）

多くの場所でロギング設定を実行できます。次の表を使用して、必要なオプションが設定されていることを確認します。

重要

- syslog の設定を行う場合、特に他の設定から継承したデフォルトを使用する際には細心の注意が必要です。下の表に示すように、オプションの中にはすべての管理対象デバイス モデルやソフトウェア バージョンに使用できないものもあります。
- 接続ロギングを設定する際の重要な情報については、接続ロギングの章を参照してください。

設定の場所	説明と詳細情報
[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]、Threat Defense 設定ポリシー、[Syslog]	このオプションは、Firewall Threat Defense デバイスにだけ適用されます。 ここで行う設定は、アクセス コントロール ポリシーのロギング設定に指定でき、この表の残りのポリシーとルールに使用するか、それらをオーバーライドできます。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）]	ここで行う設定は、この表の残りの行で指定する場所の子孫のポリシーおよびルールにあるデフォルトをオーバーライドしない限り、すべての接続イベントとセキュリティ インテリジェンス イベントの syslog のデフォルト設定になります。 Firewall Threat Defense デバイスの推奨設定：Threat Defense プラットフォーム設定を使用します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。 その他のすべてのデバイスに必要な設定：syslog アラートを使用します。 syslog アラートを指定する場合は、Syslog アラート応答の作成を参照してください。 [ロギング（Logging）] タブの設定に関する詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ルール（Rules）]、[デフォルトアクション（Default Action）]行、**ロギング**（）	ロギングのアクセス コントロール ポリシーに関連付けられているデフォルト アクションを設定します。 Cisco Secure Firewall Management Center デバイス構成ガイドおよびポリシーのデフォルト アクションによる接続のロギングでロギングに関する情報を参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ルール（Rules）]、<各ルール>、[ロギング（Logging）]	特定のルールの設定をアクセス制御ポリシーにログインします。 ログ方法の詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[セキュリティ インテリジェンス（Security Intelligence）]、**ロギング**（）	セキュリティ インテリジェンス ブロック リストのロギング設定。 次のボタンをクリックして設定します。 • [DNS ブロック リスト ロギング オプション（DNS Block List Logging Options）] • [URL ブロック リスト ロギング オプション（URL Block List Logging Options）] • [ネットワーク ブロック リスト ロギング オプション（Network Block List Logging Options）]（ブロックされたリスト上の IP アドレス用） Cisco Secure Firewall Management Center デバイス構成ガイド
[ポリシー（Policies）]>[SSL]、<各ポリシー>、[デフォルトアクション（Default Action）]行、**ロギング**（）	SSL ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギングを参照してください。
[ポリシー（Policies）]>[SSL]、<各ポリシー>、<各ルール>、[ロギング（Logging）]	SSL ルールのロギング設定。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、[デフォルトアクション（Default Action）]行、**ロギング**（）	プレフィルタ ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギングを参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）] > [プレフィルタ（Prefilter）]、<各ポリシー>、<各プレフィルタルール>、[ロギング（Logging）]	プレフィルタ ポリシーの各プレフィルタのロギング設定。 参照：Cisco Secure Firewall Management Center デバイス構成ガイド
[ポリシー（Policies）] > [プレフィルタ（Prefilter）]、<各ポリシー>、<各トンネルルール>、[ロギング（Logging）]	プレフィルタ ポリシーの各トンネル ルールのロギング設定。 参照：Cisco Secure Firewall Management Center デバイス構成ガイド
Firewall Threat Defense クラスタ構成の追加 syslog の設定：	Cisco Secure Firewall Management Center デバイス構成ガイドには syslog について複数の言及があります。「syslog」の章を検索してください。

侵入イベントの syslog の設定場所（FTD デバイス）

侵入ポリシーの syslog 設定はさまざまな場所で指定でき、必要に応じてアクセス コントロール ポリシーまたは FTD プラットフォーム設定、あるいはその両方から設定を継承できます。

設定の場所	説明と詳細情報
[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]、Threat Defense 設定ポリシー、[Syslog]	ここで設定した syslog の宛先は、侵入ポリシーのデフォルトとして使用可能なアクセス コントロール ポリシーの [ロギング（Logging）] タブで指定できます。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）]	侵入ポリシーに他のロギング ホストが指定されていない場合は、侵入イベントの syslog の宛先のデフォルト設定。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）] > [侵入（Intrusion）]、<各ポリシー>、[詳細設定（Advanced Settings）]、[syslog アラート（Syslog Alerting）] を有効化、[編集（Edit）] をクリック	アクセス コントロール ポリシーの [ロギング（Logging）] タブで指定した宛先以外の syslog コレクタを指定するには、侵入イベントの Syslog アラートの設定を参照してください。 [重大度（Severity）] または [ファシリティ（Facility）]、あるいはその両方を侵入ポリシーで設定されているとおりに使用する場合は、ポリシーにロギング ホストを設定する必要があります。アクセス コントロール ポリシーに指定されているロギング ホストを使用する場合は、侵入ポリシーに指定されている重大度とファシリティは使用されません。
ポリシー > アクセス制御 > ロギング > IPS 設定	IPS イベントの syslog メッセージを送信したい場合。設定したデフォルトの syslog 設定は、IPS イベントの syslog 宛先に使用されます。

侵入イベントの syslog の設定場所（FTD 以外のデバイス）

- （デフォルト）アクセス コントロール ポリシー（Cisco Secure Firewall Management Center デバイス構成ガイドsyslog アラートを指定した場合）（Syslog アラート応答の作成を参照）
- または侵入イベントの Syslog アラートの設定を参照してください。

デフォルトでは、侵入ポリシーはアクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用します。FTD 以外のデバイスに適用される設定がない場合は、FTD 以外のデバイスの syslog は送信されず、警告は表示されません。

ファイルとマルウェア イベントの syslog の設定場所

設定の場所	説明と詳細情報
アクセス コントロール ポリシーで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）]	これは、ファイルとマルウェアのイベントの syslog を送信するようにシステムを設定するための主要な場所です。 FTD プラットフォームの syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成 を参照してください。

設定の場所	説明と詳細情報
Firepower Threat Defense プラットフォーム設定で、次の手順を実行します。 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	これらの設定は、サポート対象のバージョンを実行しており、FTD プラットフォームを使用するようにアクセス コントロール ポリシーの [ロギング（Logging）] タブを設定している場合にのみ、Firepower Threat Defense デバイスにのみ適用されます。 Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
アクセス コントロール ルールで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、<各ルール>、[ロギング（Logging）]	FTD プラットフォームの syslog 設定を使用しない場合は、アラート応答も作成する必要があります。「Syslog アラート応答の作成」を参照してください。

セキュリティ イベントの syslog メッセージの分析

Firewall Threat Defense からのセキュリティ イベント メッセージの例（侵入イベント）

```
        1              2          3     4  5   6
Sep 24 13:42:01 192.168.0.81 SFIMS : %FTD-5-430001:SrcIP:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994, DstPort: 445,
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Revision: 2,
Message: "DCE2_EVENT__SMB_INVALID_DSIZE", Classification:
Potentially Bad Traffic, User: No Authentication Required,
Client: NetBIOS-ssn (SMB) client, ApplicationProtocol: NetBIOS-
ssn (SMB), ACPolicy: test, NAPPolicy: Balanced Security and
Connectivity, InlineResult: Blocked
```

表 *1*: セキュリティ イベントの *syslog* メッセージのコンポーネント

サンプル メッセージの項目数	ヘッダー要素	説明
0	PRI	ファシリティとアラートのシビラティ（重大度）の両方を表すプライオリティ値です。Firewall Management Center プラットフォーム設定を使用して EMBLEM 形式でのロギングを有効にした場合にのみ、この値が syslog メッセージに表示されます。アクセス コントロール ポリシーの [ロギング（Logging）] タブを使用して侵入イベントのロギングを有効にすると、PRI 値が自動的に syslog メッセージに表示されます。EMBLEM 形式を有効にする方法については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。PRI の詳細については、「RFC5424」を参照してください。
1	タイムスタンプ	syslog メッセージがデバイスから送信された日付と時刻。 • （Firewall Threat Defense デバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合か、または [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] のこの形式を使用するように指定されている場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイムゾーンを示しています。 • （その他すべてのデバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイムゾーンを示しています。 • それ以外の場合は UTC タイム ゾーンの月、日、時刻になりますが、タイム ゾーンは表示されません。 [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] でタイムスタンプ設定を指定するには、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
2	メッセージが送信されたデバイスまたはインターフェイス。 ここに表示される値は次のとおりです。 • インターフェイスの IP アドレス • デバイスのホスト名 • カスタム デバイス識別子	（Firewall Threat Defense デバイスから送信された syslog 用） [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] を使用して syslog メッセージが送信された場合で、[SyslogデバイスIDの有効化（Enable Syslog Device ID）] オプションが指定されているときは、これはそのオプションの [Syslog設定（Syslog Settings）] に設定されている値になります。 それ以外の場合、この要素はヘッダーには表示されません。 [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] でこの設定を指定するには、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
3	カスタム値	アラート応答を使用してメッセージが送信された場合、これは、メッセージを送信したアラート応答に設定されている**タグ**値がある場合は、その値になります。（Syslogアラート応答の作成 を参照）。 それ以外の場合、この要素はヘッダーには表示されません。
4	%FTD	メッセージを送信したデバイスのタイプ。%FTD は Secure Firewall Threat Defense
5	重大度	メッセージをトリガーしたポリシーの syslog 設定に指定されている重要度。 シビラティ（重大度）については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Severity Levels*」またはsyslog 重大度レベルを参照してください。
6	イベント タイプ識別子	• 430001：侵入イベント • 430002：接続の開始時に記録された接続イベント • 430003：接続の終了時に記録された接続イベント • 430004：ファイル イベント • 430005：ファイル マルウェア イベント

サンプル メッセージの項目数	ヘッダー要素	説明
--	ファシリティ	セキュリティ イベントの syslog メッセージのファシリティ（26 ページ）を参照してください。
--	メッセージの残りの部分	コロンで区切られたフィールドと値。 空または不明な値のあるフィールドはメッセージから省略されます。 フィールドの説明については、次を参照してください。 • 接続およびセキュリティ関連の接続イベントフィールド。 • 侵入イベント フィールド • ファイルおよびマルウェア イベント フィールド （注） フィールド説明のリストには、syslog フィールドとイベントビューア（Firewall Management Center の Web インターフェイスの [分析（Analysis）] メニューのメニューオプション）に表示されるフィールドの両方が含まれています。syslog 経由で使用可能なフィールドはそれを示すラベルが付けられます。 イベントビューアに表示される一部のフィールドは、syslog 経由では使用できません。また、一部の syslog フィールドはイベント ビューアには含まれていません（ただし、検索を使用すると表示できる場合があります）。また、一部のフィールドは結合されているか、または個別になっています。

セキュリティ イベントの syslog メッセージのファシリティ

一般に、セキュリティ イベントの syslog メッセージではファシリティ値は関連性がありません。ただし、ファシリティが必要な場合は、次の表を使用してください。

デバイス	接続イベントにファシリティを含める場合	侵入イベントにファシリティを含める場合	syslog メッセージ内の場所
Firewall Threat Defense	[Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] の [EMBLEM] オプションを使用します。 [Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] を使用してsyslogメッセージを送信すると、ファシリティは常に、接続イベントに対して [アラート（ALERT）] になります。	[Threat Defenseプラットフォーム設定（Threat Defense Platform Settings）] の [EMBLEM] オプションを使用するか、または侵入ポリシーのsyslog設定を使用してロギングを設定します。侵入ポリシーを使用した場合は、侵入ポリシー設定にロギング ホストも指定する必要があります。 syslog アラートを有効にし、侵入ポリシーでファシリティとシビラティ（重大度）を設定します。侵入イベントの Syslog アラートの設定を参照してください。	ファシリティはメッセージヘッダーには表示されませんが、syslog コレクタが RFC 5424、セクション 6.2.1 に基づいて値を派生させることができます。
Firewall Threat Defense 以外のデバイス	アラート応答を使用します。	侵入ポリシーの高度な設定のsyslog設定、またはアクセス コントロール ポリシーの [ロギング（Logging）] タブで識別されているアラート応答を使用します。	

詳細については、「侵入 syslog アラートの機能と重大度」および「Syslog アラート応答の作成」を参照してください。

Cisco Secure Firewall syslog メッセージのタイプ

Cisco Secure Firewall は、次の表で説明するように、複数の syslog データ タイプを送信できます。

syslog データ タイプ	参照先
Firewall Management Center からの監査ログ	syslog への監査ログのストリーミングおよび監査と Syslog の章
Firewall Threat Defense デバイスからのデバイスヘルスとネットワーク関連のログ	Cisco Secure Firewall Management Center デバイス構成ガイド

syslog データ タイプ	参照先
Firewall Threat Defense デバイスからの接続、セキュリティインテリジェンスおよび侵入イベントログ	syslog にセキュリティイベントデータを送信するためのシステムの設定について （12 ページ）。
クラッシック デバイスからの接続、セキュリティインテリジェンスおよび侵入イベント ログ	syslog にセキュリティイベントデータを送信するためのシステムの設定について （12 ページ）
ファイルおよびマルウェアのイベントのログ	syslog にセキュリティイベントデータを送信するためのシステムの設定について （12 ページ）
IPS 設定	「IPS イベントの Syslog メッセージを送信する」。 侵入イベントの syslog の設定場所（FTD デバイス） （21 ページ）

セキュリティ イベントの syslog の制限事項

- syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。
- syslog コレクタにイベントを表示するには最大 15 分かかる場合があります。
- 次のファイルおよびマルウェアのイベントのデータは syslog 経由で使用できません。
  - レトロスペクティブ イベント
  - エンドポイント向け AMP によって生成されたイベント

eStreamer サーバー ストリーミング

Event Streamer（eStreamer）を使用すると、Secure Firewall Management Center からの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、『*Secure Firewall Management Center Event Streamer Integration Guide*』と『』[英語] を参照してください。

eStreamer サーバーとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバーを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザーインターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバーが送信できるイベント タイプを制御できます。

表 *2 : eStreamer* サーバーで送信可能なイベント タイプ

イベント タイプ	説明
侵入イベント	管理対象デバイスによって生成される侵入イベント
侵入イベント パケット データ	侵入イベントに関連付けられたパケット
侵入イベント追加データ	HTTP プロキシまたはロード バランサ経由で Web サーバーに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ
検出イベント	ネットワーク検出イベント
相関および許可リスト（**Allow List**）イベント	相関およびコンプライアンスのallowリストイベント
インパクト フラグ アラート	Firewall Management Center によって生成されたインパクト アラート
ユーザー イベント	ユーザー イベント
マルウェア イベント	マルウェア イベント
ファイル イベント	ファイル イベント
接続イベント	モニター対象のホストとその他のすべてのホスト間のセッション トラフィックに関する情報

セキュリティ イベントの syslog と eStreamer の比較

一般に、現在 eStreamer に重大な既存イベントがない組織は、セキュリティ イベント データを外部で管理するのに eStreamer ではなく syslog を使用する必要があります。

Syslog	eStreamer
カスタマイズの必要なし	各リリースの変更に対応するには、大幅なカスタマイズと継続メンテナンスが必要
標準	専用
syslog 標準規格では、データ損失に対する保護はありません（特に UDP を使用している場合）	データ損失に対する保護
デバイスから直接送信	FMC から送信（処理オーバーヘッドが加わる）

Syslog	eStreamer
ファイルイベントとマルウェアイベント、接続イベント（セキュリティ インテリジェンス イベントを含む）、および侵入イベントをサポートします。	eStreamer サーバー ストリーミング （28 ページ）に示されているすべてのイベント タイプをサポートします。
一部のイベントデータは、FMC からのみ送信できます。eStreamer 経由でのみ送信でき、syslog 経由では送信できないデータ （30 ページ）を参照してください。	デバイスから syslog を介して直接送信することができないデータが含まれます。「eStreamer 経由でのみ送信でき、syslog 経由では送信できないデータ （30ページ）」を参照してください。

eStreamer 経由でのみ送信でき、syslog 経由では送信できないデータ

次のデータは Secure Firewall Management Center からのみ使用可能であるため、デバイスから syslog を介して送信することはできません。

- パケット ログ
- 侵入イベント追加データ イベント

  説明については、eStreamer サーバー ストリーミング （28 ページ）を参照してください。
- 統計情報と集約イベント
- ネットワーク検出イベント
- ユーザー アクティビティとログイン イベント
- 相関イベント
- マルウェア イベントの場合：
  - レトロスペクティブな判定
  - 関連する SHA に関する情報がすでにデバイスに同期されている場合を除き、脅威の名前と性質
- 次のフィールド：
  - [Impact] および [ImpactFlag] フィールド

    説明については、eStreamer サーバー ストリーミング （28 ページ）を参照してください。
  - [IOC_Count] フィールド
- ほとんどの raw ID と UUID。

  次に例外を示します。

- 接続イベントの syslog には次のものがあります。FirewallPolicyUUID、FirewallRuleID、TunnelRuleID、MonitorRuleID、SI_CategoryID、SSL_PolicyUUID、および SSL_RuleID
- 侵入イベントの syslog には、IntrusionPolicyUUID、GeneratorID、および SignatureID が含まれます。

- 以下を含むがこれらに限定されない拡張メタデータ：
  - 氏名、部署、電話番号などの LDAP によって提供されるユーザーの詳細。

    syslog では、イベントのユーザー名のみが提供されます。
  - SSL 証明書の詳細などの状態ベースの情報の詳細。

    syslog は、証明書のフィンガープリントなどの基本的な情報を提供しますが、cert CN など、証明書のその他の詳細は提供しません。
  - アプリケーション タグやカテゴリなどの詳細なアプリケーション情報。

    syslog はアプリケーション名のみを提供します。

  一部のメタデータ メッセージには、オブジェクトに関する追加情報も含まれています。
- 地理位置情報

eStreamer イベントタイプの選択

eStreamer サーバーで送信可能なイベントの [eStreamer イベント設定（eStreamer Event Configuration）] チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベントタイプを具体的に要求する必要があります。詳細については、*Secure Firewall Management Center Event Streamer Integration Guide* と を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

Firewall Management Center に対してこのタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 **[統合（Integration）] > [その他の統合（Other Integrations）]** を選択します。

ステップ 2 [eStreamer] をクリックします。

ステップ 3 [eStreamer イベント設定（eStreamer Event Configuration）] の下で、eStreamer サーバー ストリーミング （28 ページ）の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 4 [保存（Save）] をクリックします。

eStreamer クライアント通信の設定

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバーのピアデータベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了した後、クライアントが eStreamer サーバーに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

Firewall Management Center に対してこのタスクを実行するには、管理者または検出管理者ユーザーである必要があります。

手順

ステップ 1 **[統合（Integration）] > [その他の統合（Other Integrations）]** を選択します。

ステップ 2 [eStreamer] をクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注）
DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。

ステップ 6 [**Save**] をクリックします。
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 クライアントのホスト名の横にある[ダウンロード（download）]（  ）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある[削除（Delete）]（  ）をクリックします。

eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

Splunk でのイベント分析

（以前 Cisco Firepower App for Splunk と呼ばれていた）Cisco Secure Firewall（f.k.a. Firepower）app for Splunk を外部ツールとして使用して、Cisco Secure Firewall イベントデータを表示して操作し、ネットワーク上の脅威をハントおよび調査することができます。Splunk ツールを使用するには、eStreamer が必要です。これは高度な機能です。eStreamer サーバー ストリーミング（28 ページ）を参照してください。詳細については、「User Guide for Cisco Secure Firewall (f.k.a. Firepower) App for Splunk」を参照してください。

IBM QRadar でのイベント分析

IBM QRadar 向けの Cisco Firepower アプリケーションをイベントデータを表示するための代替手段として使用して、ネットワークへの脅威の分析、ハント、および調査をすることができます。

eStreamer が必要です。これは高度な機能です。eStreamer サーバー ストリーミング （28 ページ）を参照してください。

詳細については、「https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html」を参照してください。

外部ツールを使用したイベント データの分析の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Cisco Security Cloud Sign On アカウントを使用して、Management Center を Cisco Security Cloud に登録します。	7.6.0	任意（Any）	Cisco Security Cloud Sign On アカウントと CDO テナントを使用して、Management Center の Cisco Security Cloud への登録を許可できるようになりました。Management Center を Cisco Security Cloud に登録すると、Cisco AI Assistant for Security、Policy Analyzer & Optimizer、Zero-Touch Provisioning などの最新の Cisco Cloud サービスにアクセスできます。 新規/変更された画面：**[統合（Integration）]** > **[Cisco Security Cloud]**。 **アップグレードの影響**：Cisco Security Cloud 統合は、デフォルトで無効に設定されています。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
廃止：SecureX リボン	すべて	すべて	SecureX リボンは廃止されました。 Firefox ブラウザに [Cisco SecureXリボン（Cisco SecureX Ribbon）] ブラウザ拡張機能をインストールし、Firewall Management Center の使用中に互換性エラーが発生した場合は、 SecureX リボン拡張機能を削除してください。 拡張機能を削除するには、Firefox を開き、ブラウザのアドオンまたは拡張機能マネージャに移動し、[Cisco SecureXリボン（Cisco SecureX Ribbon）] 拡張機能を見つけて削除するか無効化にします。Firefox を再起動し、変更を適用します。
廃止：SecureX との統合	7.6.0	任意（Any）	SecureX との統合は廃止されました。Cisco Security Cloud Sign-On アカウントと Security Cloud Control テナントを使用して、Firewall Management Center とその管理対象デバイスを Cisco Security Cloud に登録できるようになりました。 新規/変更された画面：**[統合（Integration）]** > **[Cisco Security Cloud]**。 廃止された画面：**[統合（Integration）]** > **[SecureX]**
SecureX のリボン	7.0	任意（Any）	SecureX のリボンは SecureX にピボットされ、シスコのセキュリティ製品全体の脅威の状況を即座に確認できます。 Firewall Management Center で SecureX のリボンを表示するには、https://cisco.com/go/firepower-securex-documentation で『*Firepower and SecureX Integration Guide*』を参照してください。 新規/変更されたページ：新規ページ：**[システム（System）]**>**[SecureX]**
すべての接続イベントを Cisco Cloud に送信する	7.0	任意（Any）	優先順位の高い接続イベントだけでなく、すべての接続イベントを Cisco Cloud に送信できるようになりました。 新規/変更された画面：**[システム（System）]**>**[統合（Integration）]**>**[クラウドサービス（Cloud Services）]** ページ の新しいオプション

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Secure Network Analytics でデータを表示するためのクロス起動	6.7	いずれか	この機能では、[分析（Analysis）] > [コンテキストクロス起動（Contextual Cross-Launch）] ページで Secure Network Analytics アプライアンスの複数のエントリをすばやく作成する方法が導入されています。 これらのエントリを使用すると、関連するイベントを右クリックして Secure Network Analytics をクロス起動し、クロス起動したデータポイントに関連する情報を表示できます。 新しいメニュー項目：**[システム（System）]**>**[ロギング（Logging）]**>**[セキュリティ分析とロギング（Security Analytics and Logging）]** Secure Network Analytics へのイベント送信を設定する新しいページ。
追加のフィールドタイプからのコンテキストクロス起動	6.7	いずれか	次のイベントデータの追加タイプを使用して、外部アプリケーションに相互起動できるようになりました。 • アクセス コントロール ポリシー • 侵入ポリシー • アプリケーションプロトコル • クライアント アプリケーション • Web アプリケーション • ユーザー名（レルムを含む） 新しいメニューオプション：[分析（Analysis）] メニューの下のページで、ダッシュボードウィジェットおよびイベントテーブルのイベントに関して上記のデータタイプを右クリックすると、コンテキストクロス起動オプションが使用できるようになりました。 サポートされているプラットフォーム： Secure Firewall Management Center
IBM QRadar との統合	6.0 以降	任意（Any）	IBM QRadar ユーザーは、新しい Firepower 固有のアプリを使用してイベントデータを分析できます。 どの機能を使用できるかは、Firepower のバージョンによって異なります。 IBM QRadar でのイベント分析 （33 ページ）を参照してください。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
と統合するための拡張機能 SecureX Threat Response	6.5	任意（Any）	• 地域的なクラウドをサポートします。 • 米国（北米） • 欧州 • 追加イベント タイプのサポート： • ファイルおよびマルウェアのイベント • 優先順位の高い接続イベント これらは、次に関連する接続イベントです。 • 侵入イベント • セキュリティ インテリジェンス イベント • ファイルおよびマルウェアのイベント 変更された画面：**[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）]**の新規オプション。 サポートされるプラットフォーム：直接統合または syslog を介して、このリリースでサポートされているすべてのデバイス。
Syslog	6.5	任意（Any）	[AccessControlRuleName] フィールドが、侵入イベントの syslog メッセージで使用できるようになりました。
Cisco Security Packet Analyzer との統合	6.5	任意（Any）	この機能はサポートされなくなりました。
SecureX Threat Response との統合	6.3（syslog 経由、プロキシ コレクタを使用） 6.4（直接）	任意（Any）	SecureX Threat Response の強力な分析ツールを使用し、Firepower 侵入イベントデータを他のソースのデータと統合して、ネットワーク上の脅威を統合ビューに表示します。 変更された画面（バージョン 6.4）：**[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）]**の新規オプション。 サポートされるプラットフォーム：バージョン 6.3（syslog 経由）または 6.4 を実行している Secure Firewall Threat Defense デバイス

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ファイルとマルウェアのイベントの syslog サポート	6.4	任意（Any）	完全修飾ファイルおよびマルウェアのイベントデータが syslog 経由で管理対象デバイスから送信できるようになりました。 変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセス制御（Access Control）]** > **[ロギング（Logging）]**。 サポート対象プラットフォーム：バージョン 6.4 を実行している管理対象のすべてのデバイス
Splunk との統合	すべての 6.x バージョンのサポート	任意（Any）	Splunk のユーザーは、新しい個別の Splunk アプリケーションである Cisco Secure Firewall（f.k.a. Firepower）app for Splunk を使用してイベントを分析できます。 どの機能を使用できるかは、Firepower のバージョンによって異なります。 Splunk でのイベント分析 （33 ページ）を参照してください。
Cisco Security Packet Analyzer との統合	6.3	任意（Any）	導入された機能：Cisco Security Packet Analyzer にイベントに関連するパケットについてすぐにクエリを実行した後、クリックして Cisco Security Packet Analyzer の結果を調べるか、またはダウンロードして別の外部ツールで分析します。 新規画面： **[システム（System）]** > **[統合（Integration）]** > **[パケットアナライザ（Packet Analyzer）]** **[分析（Analysis）]** > **[詳細（Advanced）]** > **[パケット アナライザのクエリ（Packet Analyzer Queries）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページのイベントおよび [分析（Analysis）] メニューのページのイベント テーブルを右クリックしたときの**[クエリ（Query）]** > **[パケット アナライザ（Packet Analyzer）]**のメニュー項目 サポートされるプラットフォーム Secure Firewall Management Center

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
コンテキストクロス起動	6.3	任意（Any）	導入された機能：イベントを右クリックし、事前に定義されているか、またはカスタム URL ベースの外部リソースの関連情報を検索します。 新規画面：**[分析（Analysis）] > [詳細（Advanced）] > [コンテキストクロス起動（Contextual Cross-Launch）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニュー ページのイベント テーブルを右クリックしたときに表示される複数のオプション サポートされるプラットフォーム Secure Firewall Management Center
接続イベントと侵入イベントの syslog メッセージ	6.3	任意（Any）	統合され、簡略化された新しい設定を使用して、完全修飾接続および侵入イベントを外部ストレージおよびツールに syslog 経由で送信する機能。メッセージ ヘッダーが標準化されてイベント タイプ識別子が組み込まれ、メッセージが小型になりました。これは、不明な値や空の値が含まれたフィールドが省略されるためです。 サポート対象プラットフォーム： • すべての新機能：バージョン 6.3 を実行している Firewall Threat Defense デバイス。 • 一部の新機能：バージョン 6.3 を実行している Firewall Threat Defense 以外のデバイス。 • 少数の新機能：6.3 よりも前のバージョンを実行しているすべてのデバイス。 詳細については、セキュリティイベントの syslog メッセージの送信について （11 ページ）のトピックとサブトピックを参照してください。
eStreamer	6.3	任意（Any）	eStreamer の内容をホストのアイデンティティ ソースに関する章からこの章に移動し、eStreamer と syslog を比較した概要を追加しました。

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。