ASA FirePOWER レポートの使用

ネットワーク上のトラフィックを分析するため、さまざまな期間のレポートを表示できます。レポートは、ネットワーク トラフィックのさまざまな側面の情報を集計します。ほとんどの場合、一般情報から特定の情報にドリルダウンできます。たとえば、すべてのユーザのレポートを表示し、次に特定のユーザの詳細を表示できます。

概要レポートと詳細レポートには、トップ ポリシーや Web カテゴリなど、複数のレポート コンポーネントがあります。これらのレポートには、表示しているレポートのそのタイプで最も発生頻度の高い項目が示されます。たとえば、特定のユーザの詳細レポートを表示している場合、トップ ポリシーにはそのユーザに最も関連付けられたポリシー ヒットが表示されます。

使用可能なレポートについて

ライセンス：任意

使用可能なレポートには、ASA FirePOWER モジュールで使用可能なメイン レポートが含まれます。それらのレポートは、[ASA FirePOWER Reporting] メニューから表示できます。

一般に、名前、[View More] リンクなど、多くの項目をクリックして、個々の項目または監視するカテゴリ全体に関する詳細な情報を取得できます。

Network Overview

このレポートには、ネットワークのトラフィックに関するサマリー情報が表示されます。この情報は、詳細な分析を必要とするエリアの識別、またはネットワークが一般的な予期内で動作していることの確認に使用します。

Users

このレポートには、ネットワークの上位ユーザが表示されます。アクティブ認証に失敗したユーザは、ユーザ レポートのユーザ名 ANONYMOUS の下に表示されます。ただし、ゲスト アクセスを有効にしてる場合には、ユーザ名が Guest となります。認証の必要がないためマッ

ピングをもたないユーザは、IPアドレスで表示されます。この情報は、ユーザの異常活動の識別に役立ちます。

ヒント　ユーザ名は、ユーザの ID 情報がトラフィック フローに関連付けられている場合に限り使用できます。ユーザ ID が大多数のトラフィックのレポートで使用できるようにする場合は、アクセス コントロール ポリシーでアクティブ認証を使用する必要があります。

Applications

このレポートには、侵入イベントをトリガーしたトラフィックで検出されたHTTP トラフィックの内容または要求されたURL を表すアプリケーションが表示されます。モジュールがHTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、モジュールはここで一般的な Web ブラウジング指定を提供することに注意してください。

Web categories

このレポートには、訪問する Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトのカテゴリ（ギャンブル、広告、検索エンジン、ポータルなど）が表示されます。ユーザが訪問する上位カテゴリを識別し、アクセス コントロール ポリシーによって望ましくないカテゴリが十分にブロックされているかどうかを判別するために、この情報を使用します。

Policies

このレポートには、アクセス コントロール ポリシーがネットワークのトラフィックにどのように適用されたかが表示されます。ポリシーを削除した場合、名前に「-DELETED」が付きます。この情報を使用すると、ポリシーの効果の評価に役立ちます。

Ingress zones

このレポートには、イベントをトリガーしたパケットの入力セキュリティ ゾーンが表示されます。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

Egress zones

インライン展開環境の場合、このレポートには、イベントをトリガーとして使用したパケットの出力セキュリティ ゾーンが表示されます。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

Destinations

このレポートには、ネットワーク トラフィックの分析に基づいて、ネットワークで使用中のアプリケーション（Facebook など）が表示されます。この情報を使用すると、ネットワークで使用された上位アプリケーションの識別に役立ち、不要なアプリケーションの使用量を減らすために追加のアクセス コントロール ポリシーが必要かどうかを判断できます。

Attackers

このレポートには、イベントをトリガーした送信元ホストが使用する送信元 IP アドレスが表示されます。

Targets

このレポートには、イベントをトリガーした受信ホストが使用する宛先 IP アドレスが表示されます。

Threats

このレポートには、ネットワークに対し検出された各脅威に割り当てられた固有の識別番号と説明のテキストが表示されます。

Files logs

このレポートには、検出されたファイルのタイプ（たとえばHTMLやMSEXE）が表示されます。

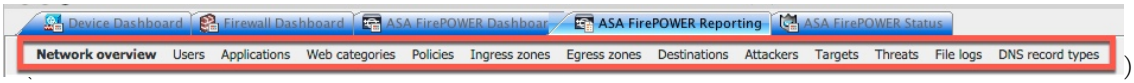
レポートの基本

ライセンス: 任意

ここでは、レポート使用の基本を説明します。以降のトピックは、いずか1つの特定のレポートではなくレポート全般に適用されます。

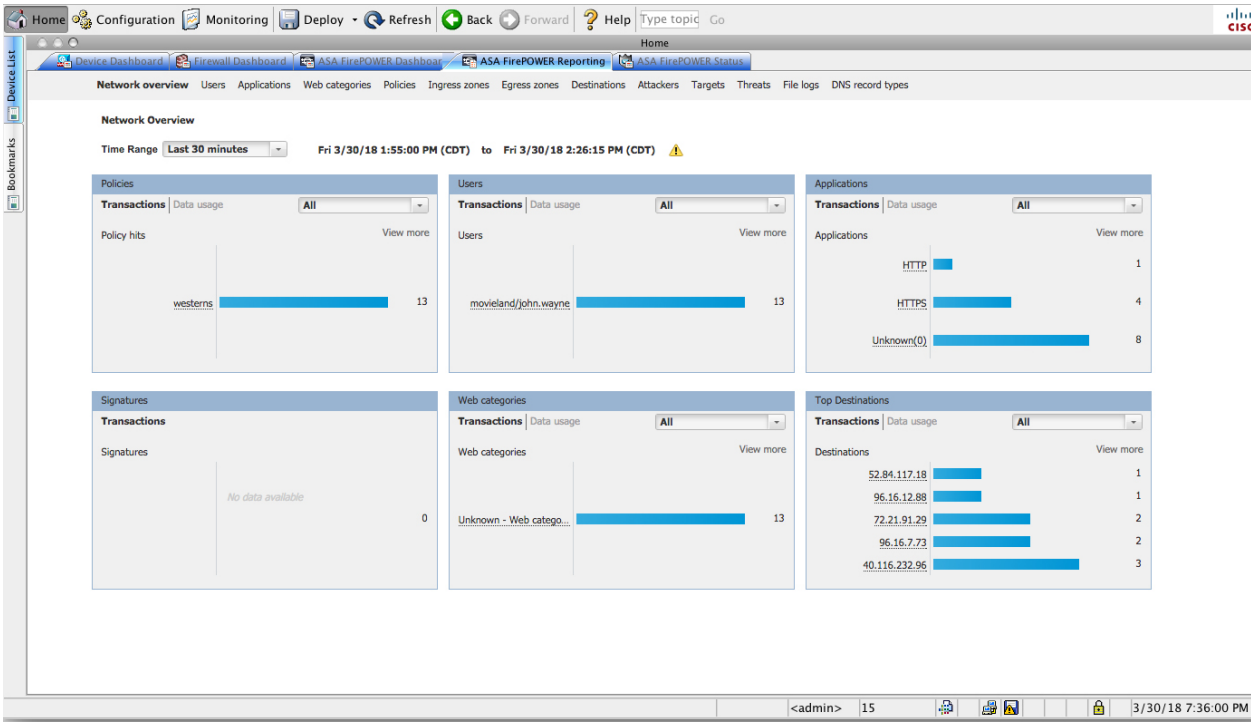
レポートを使用する前に

レポートを実行するには、ASA FirePOWER モジュールにログインして、[ホーム（Home）] > [ASA FirePOWER レポート（ASA FirePOWER Reporting）] をクリックします。使用可能なレポートのタイプは、次の図



に示すように、ウィンドウの上部に表示されます。

ネットワークの概要レポートの例を次に示します。



の詳細情報を取得するには、任意の下線付きテキストをクリックします。

レポート データについて

ライセンス: 任意

レポートデータはデバイスからすぐに収集されるため、レポートに反映されるデータとネットワーク活動の間に時差はほとんどありません。ただし、データを分析するときは次の点に注意してください。

- データは、ASA FirePOWER モジュールに適用されたアクセス コントロール ポリシーに一致するトラフィックについて収集されます。
- データは 5 分バケットで集約されるため、30 分グラフと 1 時間グラフではデータ ポイントは 5 分刻みで表示されます。1 時間の終了時に、5 分バケットが 1 時間バケットに集約され、さらにこれらが日バケットおよび週バケットに集約されます。5 分バケットは 7 日間保持され、1 時間バケットは 31 日間、日バケットは最大 365 日間保持されます。前にさかのぼるほど、データはさらに集約されます。古いデータを照会する場合、これらのデータ バケットが利用できる状態に合わせてクエリーを実行すると最良の結果が得られます。日計算はすべて UTC 時刻に基づきます。サーバやクライアントの時刻は無視されます。

（注） たとえば、5 分間よりも長い間デバイスが到達不能になったなどの理由により、データ ポイントが欠けている場合は、折れ線グラフが途切れます。

レポートのドリルダウン

ライセンス: 任意

レポートには、必要な情報にドリルダウンするための多くのリンクが含まれます。項目の上にマウスを置くと、どの項目でその詳細に進めるかがわかります。

たとえば、一般的なレポート項目において、[View More] リンクをクリックすると、その項目のサマリー レポートに移動できます。

サマリー レポートの項目をクリックして、特定の項目の詳細レポートに移動することもできます。たとえば、アプリケーション サマリー レポートで Hypertext Transfer Protocol (HTTP)をクリックすると、HTTP のアプリケーション詳細レポートに進みます。

レポート時間範囲の変更

ライセンス: 任意

レポートを表示するときは、[Time Range] リストを使用して、レポートに含める情報を定義する時間範囲を変更できます。時間範囲のリストは各レポートの上部に表示され、これを使用して最近 1 時間または 1 週間などの定義済みの時間範囲を選択したり、特定の開始時刻と終了時刻でカスタムの時間範囲を定義できます。選択した時間範囲は、選択を変更するまで、表示する他のすべてのレポートに引き継がれます。

レポートは 10 分ごとに自動的に更新されます。

ヒント モジュールの時間は、ご使用のワークステーションで設定されているタイムゾーンではなく、デバイスで定義されているタイム ゾーンに基づきます。

表 *1*: レポートの時間範囲

時間範囲	戻されるデータ
直近の 30 分（Last 30 minutes）	5 分間隔で 30 分間と、追加で最大 5 分間。
過去 1 時間（Last hour）	5 分間隔で 60 分間と、追加で最大 5 分間。
直近の 24 時間（Last 24 hours）	直前の時間境界に丸めた、1 時間間隔で最近 24 時間。たとえば、現在時刻が 13:45 の場合、[Last 24 Hour] は昨日の 13:00 から今日の 13:00 までの期間になります。
過去 7 日（Last 7 days）	直前の時間境界に丸めた、1 時間間隔で最近 7 日間。
過去 30 日（Last 30 days）	直前の午前 0 時から始まり、1 日間隔で最近 30 日間。

時間範囲	戻されるデータ
カスタム範囲（Custom Range）	ユーザ定義の時間範囲。開始日、開始時刻、終了日、および終了時刻用に [Edit] ボックスが表示されます。各ボックスをクリックして、目的の値を選択します。作業が完了したら、[Apply] をクリックしてレポートを更新します。 カスタム時間範囲を作成する際、その範囲をデータ バケットの利用可能な範囲に揃える必要があります。過去 7～31 日の範囲の場合、クエリーを時に合わせます。古い範囲の場合は、その日に合わせます。1 年を超える範囲の場合は、週に合わせます。いずれの場合も、UTC 時間を使用して日の境界を規定します。クエリー、サーバ、クライアントの時間帯は、データ バケットに関連しません。たとえば、時間帯が太平洋夏時間（PDT）で、40 前からのデータをクエリーする場合、UTC（PDT に対して 8 時間のオフセット）に合わせて、Day 1 の 4PM、Day 2 の 4PM を使用します。

レポートに表示されるデータの制御

ライセンス：任意

概要レポートと詳細レポートには、トップ ポリシーや Web カテゴリなど、複数の下位レポートがあります。各レポートパネルにあるコントロールを使用すると、データのさまざまな側面を表示できます。次のコントロールを使用できます。

[Transactions] または [Data Usage]

これらのリンクをクリックすると、トランザクション数またはトランザクションのデータ量に基づいたグラフが表示されます。

[All]、[Denied]、[Allowed]

各レポートの右上にあるラベルのないリストに、これらのオプションがあります。これらを使用して、拒否接続のみ、許可接続のみ、あるいは拒否または許可にかかわらずすべての接続の表示に変更します。

[View More]

表示する項目のレポートに移動するには、[View More] リンクをクリックします。たとえば、[Destinations] レポートの [Web Categories] グラフで [View More] をクリックすると、[Web Categories] レポートに進みます。詳細レポートのレポートを表示している場合は、詳細を表示している項目の詳細な [Web Categories] レポートに移動します。

レポート カラムについて

ライセンス：任意

通常、レポートにはグラフ形式で表示される情報の加えて、情報を提供する1つ以上のテーブルが含まれています。

- 多くのカラムの意味は、そのカラムを含むレポートによって変わります。たとえば、トランザクションのカラムには、レポートの基準になる項目タイプのトランザクション数が示されます。[Values] または [Percentages] をクリックすることで、未処理の数値で行うか、項目に報告されたすべての未処理値の比率で行うか、値の切り替えを行うこともできます。
- カラム ヘッダーをクリックすると、カラムのソート順を変更できます。

次の表に、各種レポートで使用される標準のカラムの説明を示します。標準カラムはすべてのレポートにあり、可変カラムはその項目のレポートのみに表示されます。

表 *2:* レポート カラム

カラム	説明
Transactions	報告された項目のトランザクション総数。上位レポートでは、番号がリンクになっています。表示している項目に基づいてフィルタリングされたイベントテーブルとともにイベントビューアーを表示するには、そのリンクをクリックします。表示されるイベント数がトランザクション数と異なる場合があります。これは、ディスク スペースが不足すると、新しいイベントの到着時にストレージからイベントが削除されるためであり、特に古い期間のクエリで発生します。期間が30日間前より古いクエリーは、一致するイベントを返さないことがあります。逆に、トランザクション数よりも多くのイベントが表示されることがあります。これは、項目が対象時間範囲における各5分バケットの Top N に含まれない場合、トランザクション数にそれらの期間が含まれないためです。
Transactions allowed	報告された項目で許可されたトランザクションの数。
Transactions denied	報告された項目で（ポリシーに基づいて）ブロックされたトランザクションの数。
Total bytes	報告された項目の送受信バイト数の合計。
Bytes received	報告された項目の受信バイト数。
Total Bytes Sent	報告された項目の送信バイト数。

レポートの例

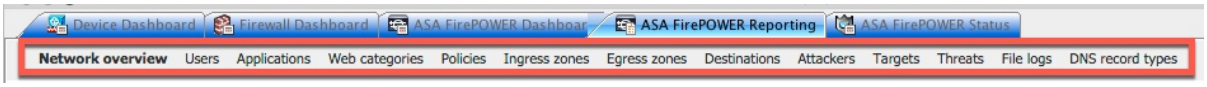
このセクションでは、ポリシー レポートを実行する方法について説明します。この手順で説明したタスクを使用して、別のレポートを実行できます。

レポートを実行するには、次の手順に従います。

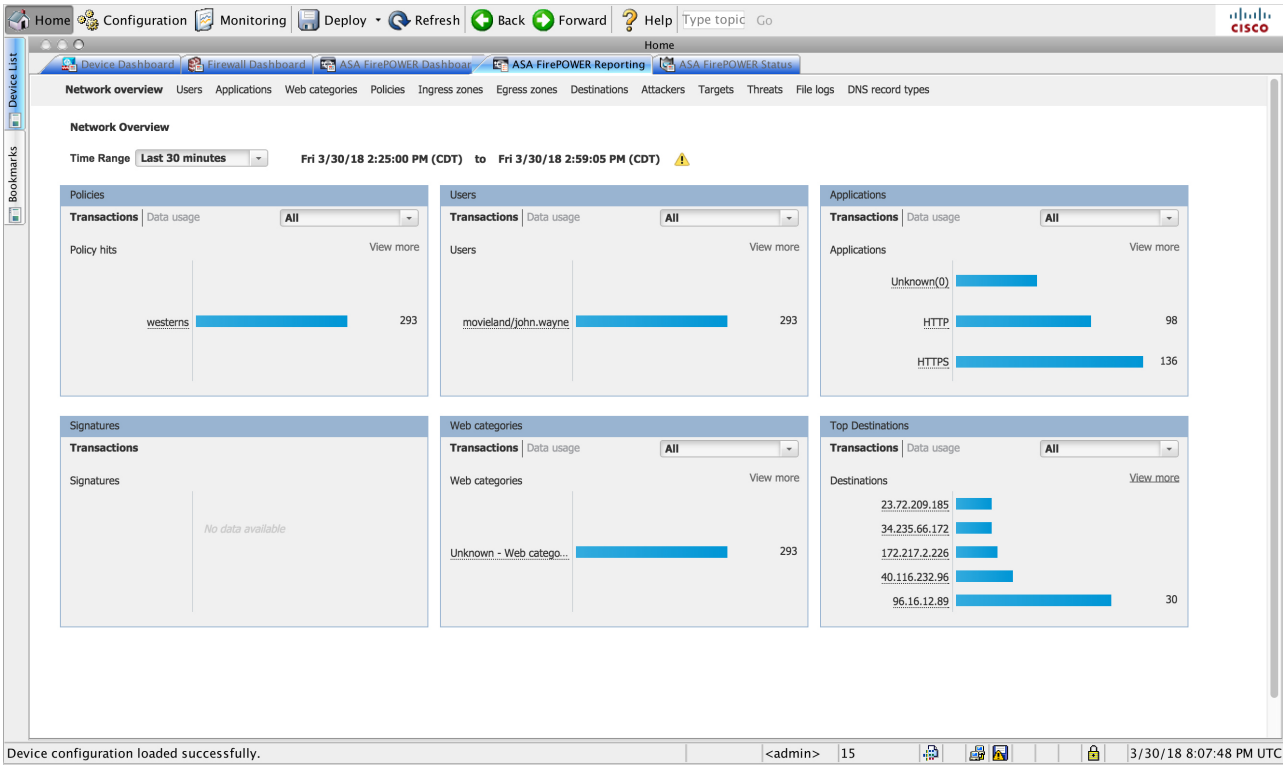
ステップ 1 ASA FirePOWER モジュールにログインします。

ステップ 2 [ホーム（Home）] > [ASA FirePOWER レポート（ASA FirePOWER Reporting）] をクリックします。

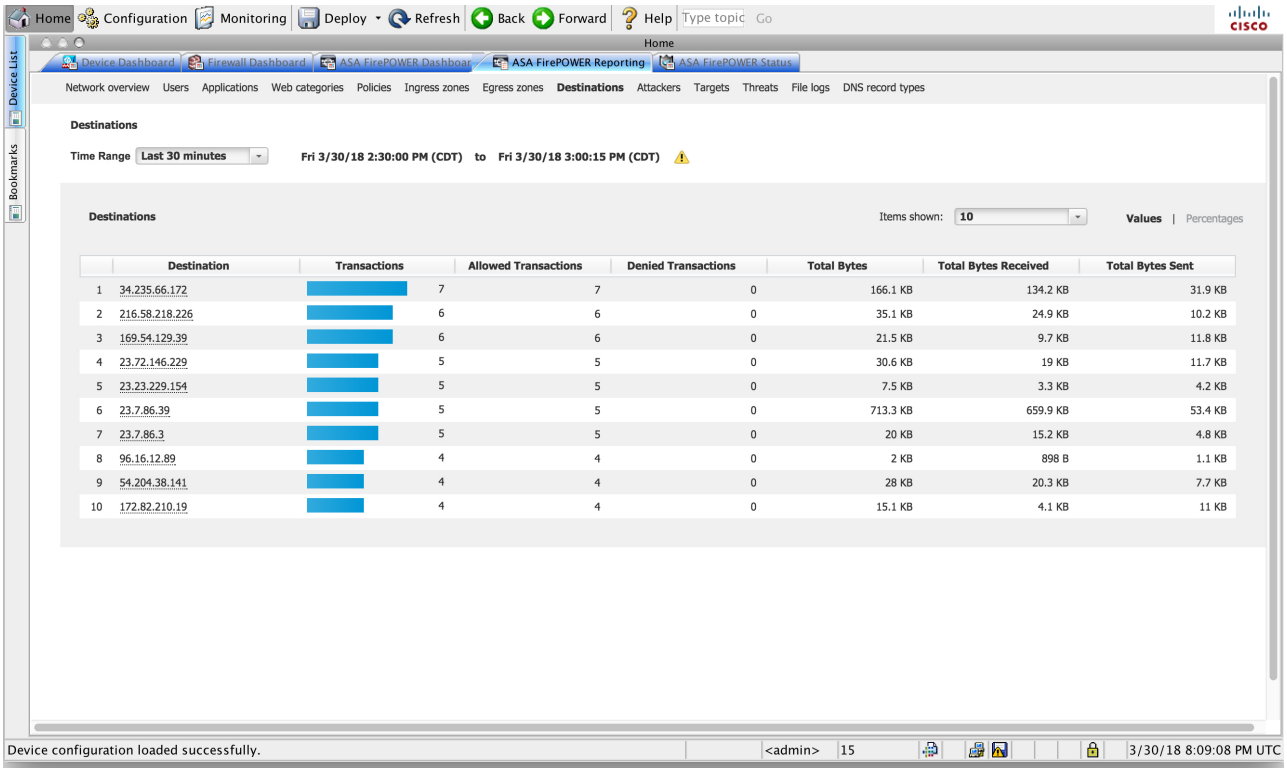
使用可能なレポートのタイプは、次の図に示すように、ウィンドウの上部に表示されます。



ステップ 3 多くのレポートで、レポートに含まれるカテゴリについての詳細を表示できます。たとえば、[ネットワークの概要（Network Overview）] をクリックします。



ステップ 4 [ネットワークの概要（Network Overview）] レポートの結果で、上位の宛先の名前をクリックして、宛先に関する詳細情報を取得します。



結果には、宛先についての概要情報と詳細が表示されます。

（オプション）[詳細情報（View More）] をクリックして、さらに詳しい情報を表示します。