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面の情報を集約します。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。

詳細については、以下を参照してください。

- 使用可能なレポートについて（41-1 ページ）
- レポートの基礎（41-3 ページ）
- レポートの例（41-7 ページ）

使用可能なレポートについて

ライセンス：任意（Any）

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。[ASA FirePOWER レポート（ASA FirePOWER Reporting）] メニューからこれらのレポートを表示できます。

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

ネットワークの概要

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測の範囲内で動作していることの確認に使用します。

ユーザ

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。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。

アプリケーション

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 カテゴリ

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。この情報は、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使用します。

ポリシー

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。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。

入力ゾーン

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。

出力ゾーン

このレポートには、イベントをトリガー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。

宛先

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。

攻撃者

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。

ターゲット

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。

ファイル ログ

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。

レポートの基礎

ライセンス：任意（Any）

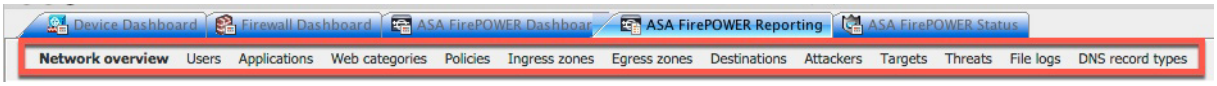
ここでは、レポート使用の基本を説明します。続く各トピックは、いずれか 1 つの特定のレポートではなく、レポート全般に適用されます。

詳細については、以下を参照してください。

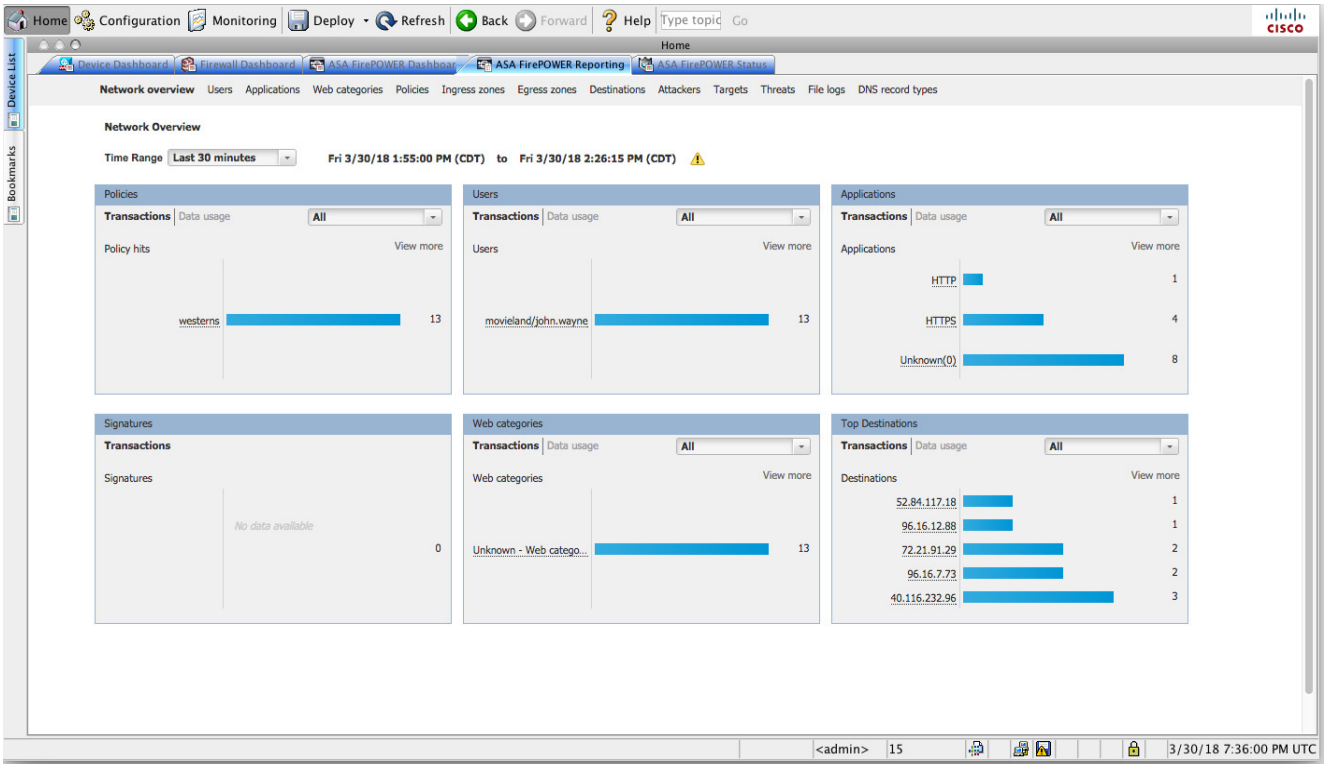
- レポートの開始（41-3 ページ）
- レポート データについて（41-4 ページ）
- レポートへのドリル（41-5 ページ）
- レポートの時間範囲の変更（41-5 ページ）
- レポートに表示されるデータの制御（41-6 ページ）
- レポート カラムについて（41-6 ページ）

レポートの開始

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。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（Any）

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。

（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。

レポートへのドリル

ライセンス:任意（Any）

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、[詳細情報（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。

レポートの時間範囲の変更

ライセンス:任意（Any）

レポートを表示するときは、[時間範囲（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したりできます。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。

次の表に、時間範囲オプションの説明を示します。

表 41-1　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 5 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 3 hours）	直前の時間境界に丸めた、1 時間間隔で直近の 24 時間。たとえば、現在時刻が 13:45 の場合、[最近の 24 時間（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 時間間隔で直近の 7 日間。
過去 30 日（Last 7 days）	直前の午前 0 時から始まり、1 日間隔で最近の 30 日間。
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 [編集（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、[適用（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。それ以前の場合は、クエリーを日に合わせます。1 年を超える範囲の場合は、クエリーを週に合わせます。

レポートに表示されるデータの制御

ライセンス:任意（Any）

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。

[トランザクション（Transactions）] または [データ使用量（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。

[すべて（All）]、[拒否（Denied）]、[許可（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。

詳細情報（View More）
表示する項目のレポートに移動するには、[詳細情報（View More）] リンクをクリックします。たとえば、[接続先（Destinations）] レポートの [Web カテゴリ（Web Categories）] グラフで [詳細情報（View More）] をクリックすると、[Web カテゴリ（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 カテゴリ（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（Any）

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。[値（Values）] または [割合（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。

表 41-2　レポート カラム

カラム（Column）	説明
トランザクション（Transactions）	報告された項目のトランザクション総数。
許可されたトランザクション（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。
拒否されたトランザクション（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。
合計バイト数（Total Bytes）	報告された項目の送受信バイト数の合計。

カラム（Column）	説明
受信バイト数（Bytes received）	報告された項目の受信バイト数。
送信バイト数（Total Bytes Sent）	報告された項目の送信バイト数。

レポートの例

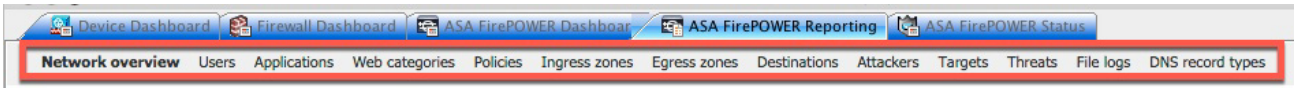
このセクションでは、ポリシー レポートを実行する方法について説明します。この手順で説明したタスクを使用して、別のレポートを実行できます。

レポートを実行するには、次の手順に従います。

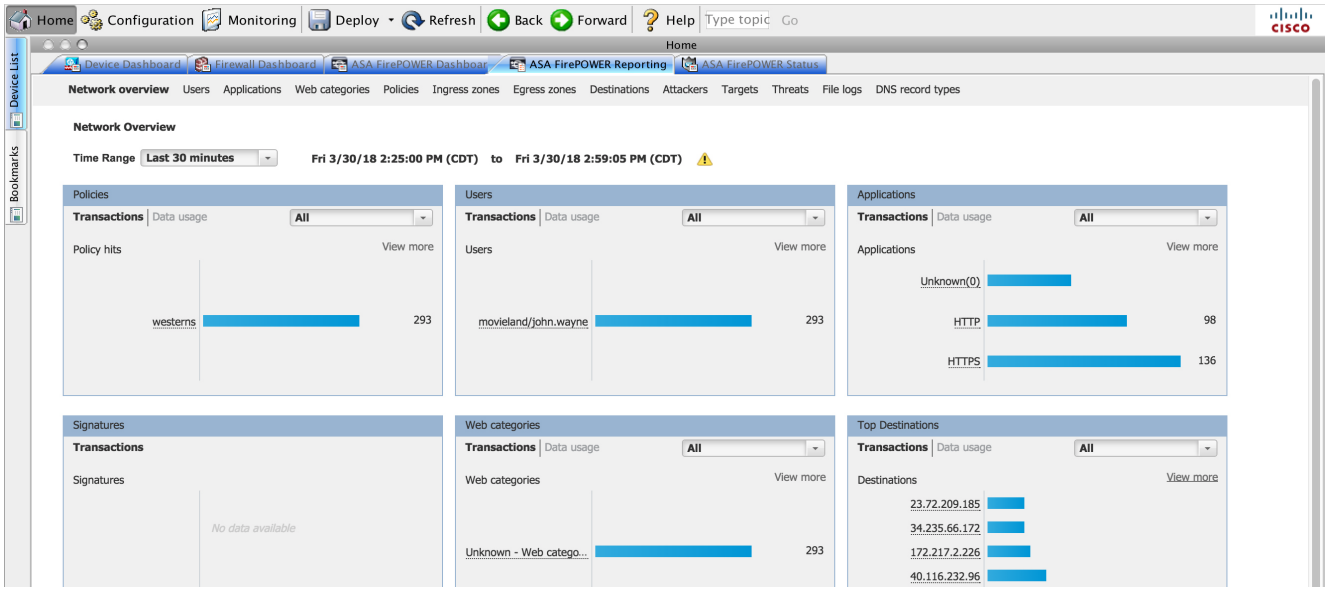
手順 1　ASA FirePOWER モジュールにログインします。

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

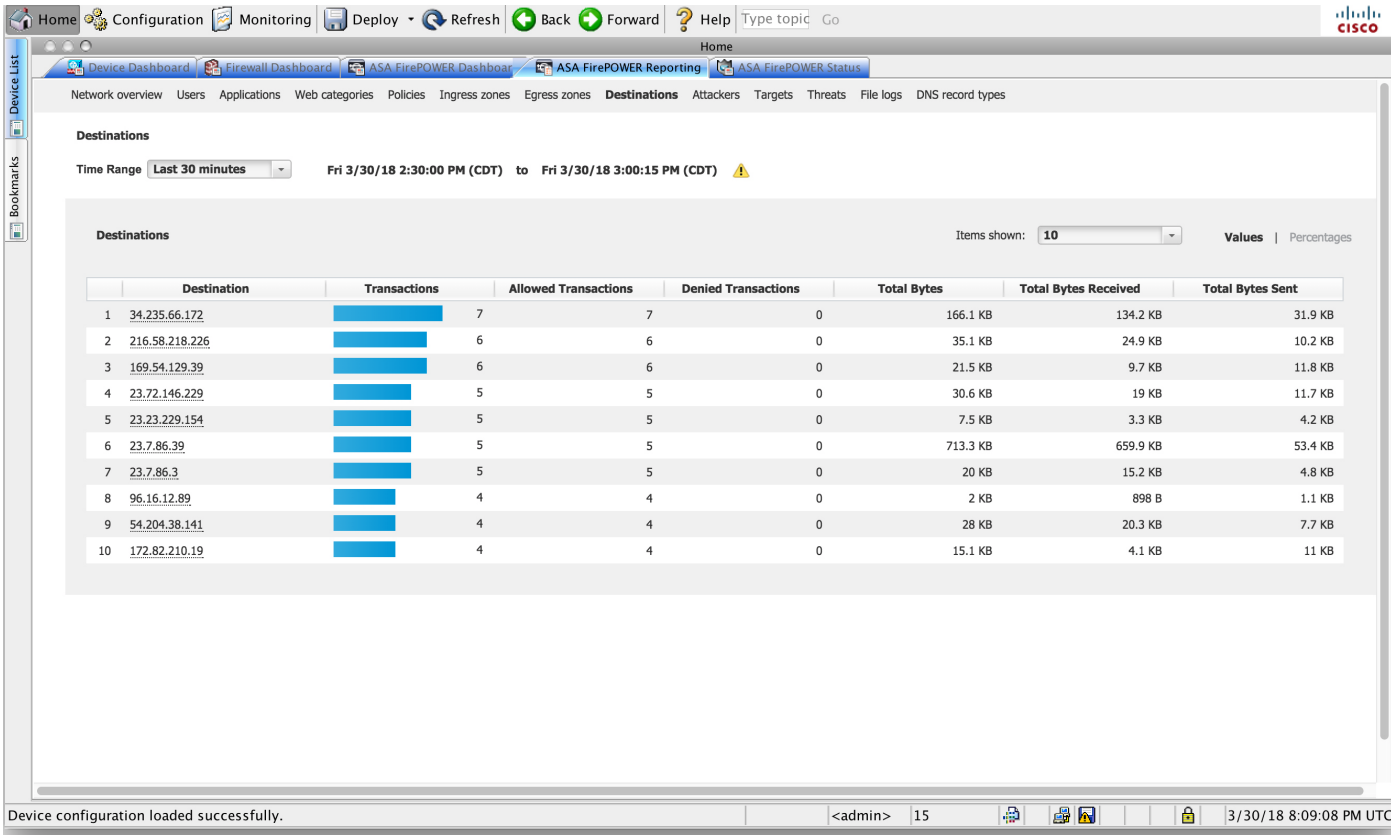
使用可能なレポートのタイプは、次の図に示すように、ウィンドウの上部に表示されます。



手順 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。



手順 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。

手順 5　（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。