トラフィック プロファイル

ここでは、トラフィック プロファイルの設定方法について説明します。

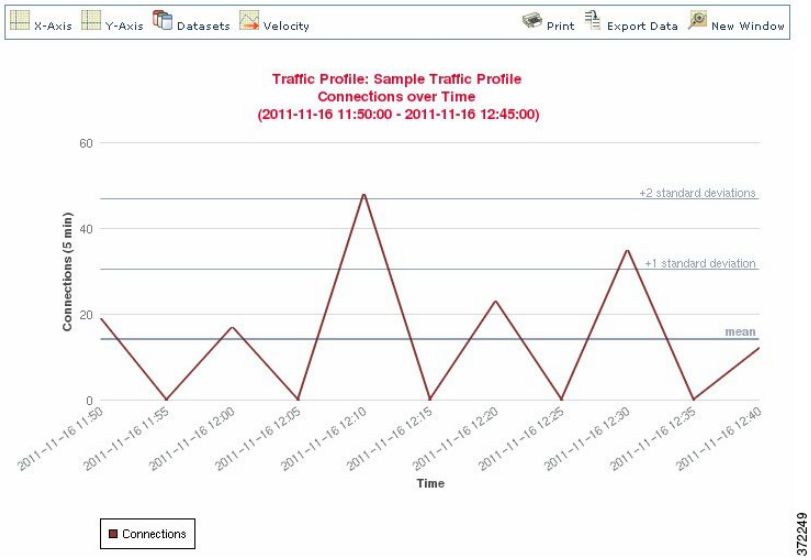
トラフィック プロファイルの概要

トラフィック プロファイルはプロファイル生成時間枠（PTW）内に収集した接続データを基に、ネットワーク トラフィックをグラフで表したものです。この測定結果が正常なネットワーク トラフィックを表しているものと推定します。学習期間が経過すると、新たなトラフィックをプロファイルに照らして評価することで異常なネットワーク トラフィックを検出します。

デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。デフォルトで、トラフィック プロファイルは5分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、このサンプリング レートは最大 1 時間間隔まで拡大することができます。

ヒント シスコは少なくとも 100 のデータ ポイントを含む PTW の設定を推奨します。統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があります。

次の図は、PTW を 1 日、サンプリング レートを 5 分としたトラフィック プロファイルを示しています。



また、トラフィック プロファイルの非アクティブ期間を設定することもできます。トラフィック プロファイルは非アクティブ期間もデータ収集を行いますが、収集したデータをプロファイル統計の計算に使用しません。トラフィック プロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

たとえば、すべてのワークステーションが毎日深夜 0:00 にバックアップされるネットワーク インフラストラクチャがあるとします。バックアップには約 30 分かかり、その間はネットワーク トラフィックが急増します。予定されたバックアップ時間に合わせてトラフィック プロファイルの非アクティブ期間を繰り返すよう設定します。

（注） システムは接続の終了データを使って接続グラフとトラフィック プロファイルを作成します。トラフィック プロファイルを使用するには、必ず Firepower Management Center データベースに接続の終了イベントをロギングしてください。

トラフィック プロファイルの実装

トラフィック プロファイルを有効にすると、システムは設定した学習期間（PTW）の間接続データを収集し、評価します。システムは学習期間が経過すると、トラフィック プロファイルを対象にした相関ルールを評価します。

たとえば、ネットワークを通過するデータ量（パケット数、KB 数、または接続数で測定）が、平均トラフィック量に比べて標準偏差の 3 倍も急激に上昇した場合、攻撃または他のセキュリティ ポリシー違反を示す可能性があると判断してトリガーするルールを作成できます。その後、このルールを相関ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。

トラフィック プロファイルの対象設定

トラフィック プロファイルは、プロファイル条件とホスト プロファイル限定による制約を受けます。

プロファイル条件を使って、すべてのネットワーク トラフィックをプロファイリングすることもできます。また、トラフィック プロファイルの対象を絞って、特定のドメイン、特定のドメイン内や複数のドメイン内のサブネット、または個別のホストをモニタすることもできます。マルチドメイン展開では次のプロファイリングが可能です。

- リーフ ドメイン管理者は、リーフ ドメイン内のネットワーク トラフィックをプロファイリングできます。
- 高位レベル ドメインの管理者は、ドメイン内または複数ドメインでトラフィックのプロファイリングができます。

また、プロファイル条件では接続データに基づく基準を設けてトラフィック プロファイルを制約することもできます。たとえば、特定のポート、プロトコル、アプリケーションが使われているセッションのみトラフィック プロファイルでプロファイリングを行うようにプロファイル条件を設定できます。

また、トラッキング対象のホストに関する情報を使用してトラフィック プロファイルを制約することもできます。この制約は、ホストプロファイル限定と呼ばれます。たとえば、重要度の高いホストに限定して接続データを収集できます。

（注） トラフィック プロファイルを高レベルのドメインに制約すると、各子孫リーフ ドメインの同じタイプのトラフィックが集約およびプロファイルされます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

関連トピック

相関ポリシーとルールの概要

トラフィック プロファイル条件

単純なトラフィック プロファイル条件とホスト プロファイル限定を作成できます。また、複数の条件の組み合わせとネストによってより複雑な構造を作成することもできます。

条件には、カテゴリ、演算子、および値という 3 つの部分があります。

- 使用できるカテゴリは、トラフィック プロファイル条件を作成しているか、それともホスト プロファイル限定を作成しているかに応じて異なります。
- 使用できる演算子は、選択したカテゴリによって異なります。
- 条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキスト フィールドに値を入力する必要があります。それ以外の場合、ドロップダウン リストから 1 つ以上の値を選択できます。

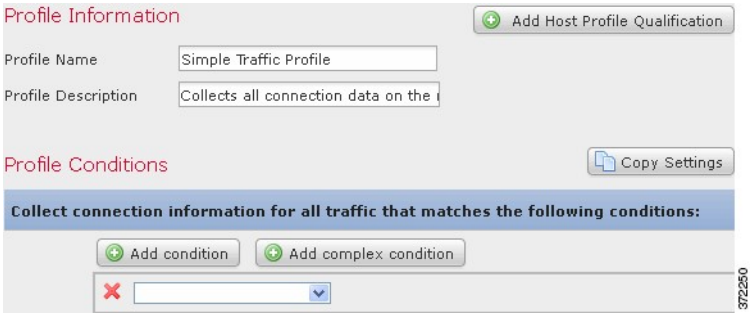
ホストプロファイル限定の場合、開始側または応答側のホストに関する情報のデータを使用して、トラフィック プロファイルに制約を適用するかどうかを指定する必要もあります。

構造に複数の条件を含める場合は、それらの条件を [および（AND）] 演算子または [または（OR）] 演算子で結合する必要があります。同じレベルにある複数の条件は、合わせて評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件を満たす必要があることを示します。
- [または（OR）] 演算子は、制御対象のレベルにある複数の条件の少なくとも 1 つが満たされている必要があることを示します。

制約が適用されていないトラフィック プロファイル

モニタ対象ネットワーク セグメント全体のデータを収集するトラフィック プロファイルを作成する場合、次の図に示すように、条件を含まない非常に単純なプロファイルを作成できます。



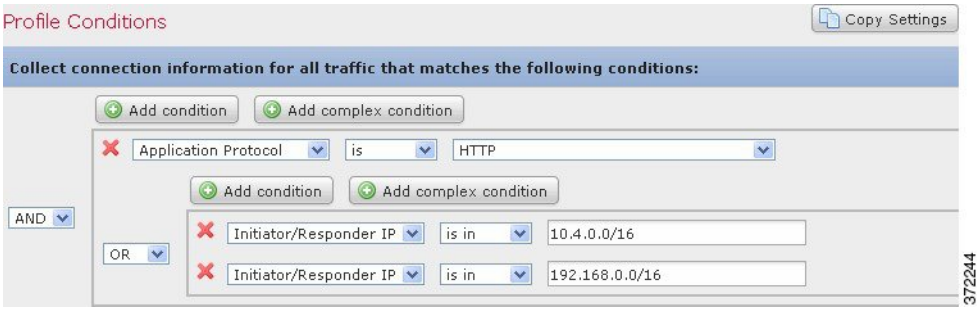
単純なトラフィック プロファイル

プロファイルに制約を適用して、1 つのサブネットのデータのみを収集するには、次の図に示すように 1 つの条件を追加できます。

複雑なトラフィック プロファイル

次のトラフィック プロファイルには、[および（AND）] で結合された 2 つの条件が含まれています。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルは接続データを収集します。この例では、特定のサブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。

一方、次のトラフィック プロファイルでは、2 つのサブネットのいずれかの HTTP アクティビティに関する接続データを収集しますが、最後は複合条件を構成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

```
(A and (B or C))
```

条件	条件で指定する内容
A	アプリケーション プロトコル名が HTTP である
B	IP アドレスが 10.4.0.0/16 内にある
C	IP アドレスが 192.168.0.0/16 内にある

トラフィック プロファイルの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

アクティブで完全なトラフィック プロファイルに対して記述されたルールのみが、相関ポリシー違反をトリガーできます。各トラフィック プロファイルの横にあるスライダ アイコンは、プロファイルがアクティブでありデータを収集しているかどうかを示します。経過表示バーは、トラフィック プロファイルの学習期間のステータスを示します。

マルチドメイン展開では、現在のドメインで作成されたトラフィック プロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの選択したトラフィック プロファイルも表示されますが、これは編集できません。下位のドメインで作成されたトラフィック プロファイルを表示および編集するには、そのドメインに切り替えます。

（注） プロファイルの条件が無関係なドメインに関する情報（名前や管理対象デバイスなど）を公開する場合、システムは先祖ドメインからのトラフィック プロファイルを表示しません。

手順

ステップ 1 **[Policies]** > **[Correlation]** を選択して、[トラフィック プロファイル（Traffic Profiles）] タブをクリックします。

ステップ 2 トラフィック プロファイルを管理します。

- アクティブ化/非アクティブ化：トラフィック プロファイルをアクティブ化または非アクティブ化するには、スライダをクリックします。トラフィック プロファイルを非アクティブ化すると、そのプロファイルに関連するデータが削除されます。プロファイルを再度アクティブ化する場合は、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。
- 作成：新しいトラフィック プロファイルを作成するには、[新規プロファイル（New Profile）] をクリックして、トラフィック プロファイルの設定 （7 ページ） で説明する手順を実行します。また、コピー アイコン（  ）をクリックして、既存のトラフィック プロファイルのコピーを編集することもできます。
- 削除：トラフィック プロファイルを削除するには、削除アイコン（  ）をクリックして、選択内容を確認します。
- 編集：既存のトラフィック プロファイルを変更するには、編集アイコン（  ）をクリックして、トラフィック プロファイルの設定 （7 ページ） で説明する手順を実行します。トラフィック プロファイルがアクティブな場合は、そのプロファイルの名前と説明のみを変更できます。
- グラフ：グラフとしてトラフィック プロファイルを表示するには、グラフアイコン（  ）をクリックします。マルチドメイン展開では、グラフが無関係なドメインに関する情報を公開する場合、先祖ドメインに属しているトラフィック プロファイルのグラフを表示できません。

トラフィック プロファイルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

トラフィック プロファイルを高レベルのドメインに制約すると、各子孫リーフ ドメインの同じタイプのトラフィックが集約およびプロファイルされます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

手順

ステップ 1 **[Policies]** > **[Correlation]** を選択し、[トラフィック プロファイル（Traffic Profiles）] タブをクリックします。

ステップ 2 [新規プロファイル（New Profile）] をクリックします。

ステップ 3 プロファイル名を入力し、オプションでプロファイルの説明を入力します。

ステップ 4 オプションで、トラフィック プロファイルを制約します。

- 設定のコピー：既存のトラフィック プロファイルから設定をコピーするには、[設定のコピー（Copy Settings）] をクリックし、使用するトラフィック プロファイルを選択して [ロード（Load）] をクリックします。
- プロファイル条件：トラッキング対象の接続の情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイル条件の追加 （8 ページ）の説明に従って続行します。
- ホスト プロファイル認定：トラッキング対象のホストの情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイルへのホスト プロファイル認定の追加 （9 ページ）の説明に従って続行します。
- プロファイルの時間帯（PTW）：プロファイルの時間帯を変更するには、時間の単位を入力し、[時間（hour(s)）]、[日（day(s)）]、または [週（week(s)）] を選択します。
- サンプリング レート：サンプリング レートを分単位で選択します。
- 非アクティブ期間：[非アクティブ期間の追加（Add Inactive Period）] をクリックし、ドロップダウン リストを使用して、トラフィック プロファイルを非アクティブなままにする日時と頻度を指定します。非アクティブなトラフィック プロファイルは、相関ルールをトリガーしません。トラフィック プロファイルでは、プロファイルの統計情報に非アクティブな期間のデータを含めません。

ステップ 5 トラフィック プロファイルを保存します。

- プロファイルを保存し、ただちにデータを収集し始めるには、[保存してアクティブにする（Save & Activate）] をクリックします。

- アクティブ化せずにプロファイルを保存するには、[保存（Save）] をクリックします。

トラフィック プロファイル条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 トラフィック プロファイル エディタの [プロファイル条件（Profile Conditions）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 2 トラフィック プロファイル条件の構文 （10 ページ） と トラフィック プロファイル条件 （3 ページ） の説明に従い、各条件のカテゴリ、演算子、値を指定します。

演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用 （14 ページ） に説明してあるように単一の条件で複数の値を選択できます。

カテゴリが IP アドレスを表している場合、演算子として [含まれる（is in）] または [含まれない（is not in）] を選択すると、IP アドレス範囲内にその IP アドレスが含まれるのか、含まれないのかを指定できます。

例

次のトラフィック プロファイルは、特定のサブネットの情報を集めます。条件のカテゴリは [イニシエータ/レスポンダ IP（Initiator/Responder IP）]、演算子は [含まれる（is in）]、値は `10.4.0.0/16` です。

関連トピック

Firepower システムの IP アドレス表記法

トラフィック プロファイルへのホスト プロファイル認定の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

手順

ステップ 1 トラフィック プロファイル エディタで、[ホスト プロファイル認定の追加（Add Host Profile Qualification）] をクリックします。

ステップ 2 [ホスト プロファイル認定（Host Profile Qualification）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

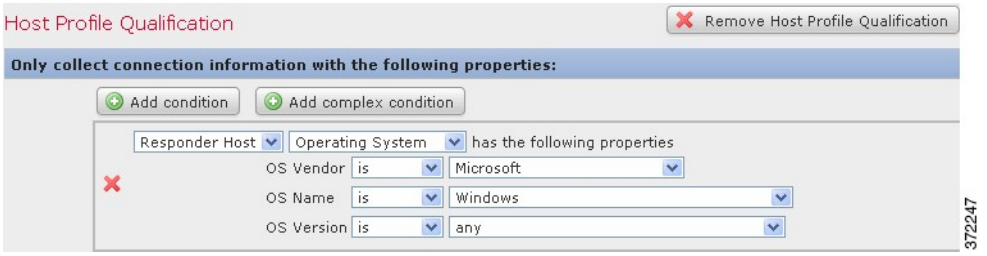
- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 3 トラフィック プロファイルのホスト プロファイル限定の構文 （11 ページ） と トラフィック プロファイル条件 （3 ページ）の説明に従い、各条件のホストタイプ、カテゴリ、演算子、値を指定します。

演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用 （14 ページ）に説明してあるように単一の条件で複数の値を選択できます。

例

次のホストプロファイル認定によりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。



トラフィック プロファイル条件の構文

次の表で、トラフィック プロファイル条件を作成する方法について説明します。トラフィック プロファイルの作成に使用可能な接続データは、トラフィックの特性と検出方法を含む複数の要因によって変わることに留意してください。

表 *1*: トラフィック プロファイル条件の構文

次を選択できます。	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
[クライアント カテゴリ（Client Category）]	クライアント カテゴリを 1 つ以上選択します。
接続タイプ	プロファイルが Firepower システムの管理対象デバイスによってモニタされるトラフィックからの接続データ、またはエクスポートされた NetFlow レコードからの接続データを使用するかどうかを選択します。 接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。
接続先（国）または送信元（国）	国を 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	IP アドレス、または IP アドレスの範囲を入力します。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

次を選択できます。	選択する演算子と内容
NetFlow デバイス	トラフィック プロファイルの作成に使用するデータの NetFlow エクスポータを選択します。
レスポンダ ポート/ICMP コード	ポート番号または ICMP コードを入力します。
セキュリティ インテリジェンス カテゴリ	セキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。 トラフィック プロファイル条件にセキュリティ インテリジェンスのカテゴリを使用するには、アクセス コントロール ポリシーでそのカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定する必要があります。
SSL 暗号化セッション	[正常に復号（Successfully Decrypted）] を選択します。
トランスポート プロトコル	トランスポート プロトコルとして **TCP** または **UDP** と入力します。
[Web アプリケーション（Web Application）]	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

接続イベント フィールドの入力の要件
Firepower システムの IP アドレス表記法

トラフィック プロファイルのホスト プロファイル限定の構文

ホスト プロファイル限定の条件を作成するときには、まず、トラフィック プロファイルを制約するために使用するホストを選択する必要があります。[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] のいずれかを選択できます。ホスト ロールを選択したら、ホスト プロファイル限定の条件の作成を続行します。

NetFlow レコードを使用してネットワーク マップにホストを追加できますが、これらのホストに関する利用可能な情報は限定されています。たとえば、これらのホストに利用可能なオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。さらに、エクスポートされた NetFlow レコードからの接続データをトラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、どのホストがレスポンダであるかを示す情報が含まれないことに注意してください。システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

暗黙的（または汎用の）クライアントを照合するには、クライアントに応答するサーバで使われるアプリケーション プロトコルに基づいてホスト プロファイル限定を作成します。接続のイニシエータ（または送信元）として機能するホスト上のクライアント リストに含まれるアプリケーション プロトコル名の後に**クライアント**が続いている場合、そのクライアントは実際に

は暗黙的クライアントである可能性があります。つまり、検出されたクライアントトラフィックに基づいてではなく、そのクライアントのアプリケーションプロトコルを使用するサーバ応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホスト上のクライアントとして**HTTPS クライアント**がシステムにより報告される場合、[アプリケーション プロトコル（Application Protocol）] を [HTTPS] に設定した [レスポンダ ホスト（Responder Host）] のホスト プロファイル限定を作成します。これは、レスポンダまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて HTTPS クライアントが汎用クライアントとして報告されるためです。

表 *2:* ホスト プロファイル限定の構文

次を選択できます。	選択する演算子と内容
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション プロトコル（Application Protocol）]	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション ポート（Application Port）]	アプリケーションプロトコルのポート番号を入力します。
[アプリケーション プロトコル（Application Protocol）] > [プロトコル（Protocol）]	プロトコルを選択します。
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
[クライアント（Client）] > [クライアント（Client）]	クライアントを 1 つ以上選択します。
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
[クライアント カテゴリ（Client Category）]	クライアント カテゴリを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
[ハードウェア（Hardware）]	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには `iPhone` と入力します。
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。
[ホスト タイプ（Host Type）]	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	IOC タグを 1 つ以上選択します。

次を選択できます。	選択する演算子と内容
[ジェイルブロークン（Jailbroken）]	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが [ARP/DHCP で検出（ARP/DHCP Detected）] されるかどうかを選択します。つまり、次のいずれかです。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
NETBIOS 名	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）] > [OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。

次を選択できます。	選択する演算子と内容
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
[Web アプリケーション（Web Application）]	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。
使用可能な任意のホスト属性（デフォルト コンプライアンス ホワイトリスト ホスト属性を含む）	選択するホスト属性のタイプに応じて、適切な値を次のように指定します。 • ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。 • ホスト属性タイプが Text の場合、テキスト値を入力します。 • ホスト属性タイプが List の場合、有効なリスト文字列を選択します。 • ホスト属性タイプが URL の場合、URL 値を入力します。

トラフィック プロファイル条件での複数の値の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をトラフィック プロファイルに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

手順

ステップ 1 トラフィック プロファイルまたはホスト プロファイルの資格条件を作成するときに、演算子として [存在する（is in）] または [存在しない（is not in）] を選択します。

ドロップダウン リストがテキスト フィールドに変わります。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。

ステップ 4 右矢印をクリックして、選択した項目を [選択済み（Selected）] に移動します。

ステップ 5 [OK] をクリックします。