ルール管理：共通の特性

以下のトピックでは、Firepower Management Center でさまざまなポリシーのルールの共通特性を管理する方法について説明します。

ルールの概要

さまざまなポリシー内のルールで、ネットワーク トラフィックをきめ細かく制御できます。システムは最初の一致のアルゴリズムを使用して、指定した順番でルールに照らし合わせてトラフィックを評価します。

これらのルールはポリシー全体で一貫していない他の設定を含んでいる場合もありますが、次のような多くの基本的な特性や設定メカニズムは共通です。

- 条件：ルールの条件は各ルールが処理するトラフィックを指定します。各ルールには複数の条件を設定できます。トラフィックがルールに一致するには、すべての条件に一致する必要があります。
- アクション：ルールのアクションによって、一致するトラフィックの処理方法が決まります。選択できる [アクション（Action）] リストがルールにない場合でも、ルールには関連付けられたアクションが 1 つある点に注意してください。たとえば、カスタム ネットワーク分析ルールはそのルールの「アクション」としてネットワーク分析ポリシーを使用します。
- 位置：ルールの位置は評価の順番を決定します。ポリシーを使ってトラフィックを評価すると、システムは指定した順序でトラフィックとルールを照合します。通常は、システムによるトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のルールに

従って行われます（トラフィック フローの追跡と記録を行うがトラフィック フローには影響しないモニタ ルールは例外です）。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

- カテゴリ：いくつかのルール タイプを整理するために、各親ポリシーでカスタムのルール カテゴリを作成できます。
- ロギング：多くのルールでは、ルールが処理する接続をシステムがロギングするかどうか、およびロギングの処理方法は、ロギングの設定によって制御されます。一部のルール（ID ルールやネットワーク分析ルールなど）にはロギング設定は含まれません。これは、ルールが接続の最終的な性質を決定するわけではなく、またそのルールが接続をロギングするために特別に設計されているわけではないためです。
- コメント：一部のルール タイプでは、変更を保存するたびにコメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ヒント 多くのポリシーエディタでは、右クリック メニューで編集、削除、移動、有効化、無効化など、数多くのルール管理オプションへのショートカットを提供しています。

共通の特性を持つルール

この章では、以下のルールや設定に見られる多くの共通の側面について説明しています。共通していない設定の情報については、以下を参照してください。

- アクセス コントロール ルール：アクセス コントロール ルール
- SSL ルール：SSL ルールの作成および変更
- DNS ルール：DNS ルールの作成および編集
- ID ルール：アイデンティティ ルールの作成
- ネットワーク分析ルール：ネットワーク分析ルールの設定
- インテリジェントアプリケーションバイパス（IAB）：インテリジェントアプリケーションバイパス
- アプリケーション フィルタ：アプリケーション フィルタ

共通の特性のないルール

次のルールの設定は、この章では説明していません。

- 侵入ルール：ルールを使用した侵入ポリシーの調整
- ファイル ルール：ファイル ルール
- 相関ルール：相関ルールの設定

- NAT ルール（クラシック）：7000 および 8000 シリーズ デバイス用の NAT
- 8000 シリーズ ファスト パス ルール：高速パス ルールの設定（8000 シリーズ）

ルール条件タイプ

次の表は、この章に記述している一般的なルールの条件について説明し、使用設定を列挙します。

条件	トラフィック制御方法	対応しているルール/設定
セキュリティ ゾーンの条件，（5 ページ）	送信元と宛先のセキュリティ ゾーン	アクセス コントロール ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
ネットワーク条件，（6 ページ）	送信元 IP アドレスと宛先 IP アドレス、対応している場合には地理的な場所や発信側のクライアント	アクセス コントロール ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
VLAN 条件，（8 ページ）	VLAN タグ	アクセス コントロール ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
ポートおよびICMP コードの条件，（9 ページ）	送信元ポート、宛先ポート、プロトコル、ICMP コード	アクセス コントロール ルール SSL ルール アイデンティティ ルール
アプリケーション条件（アプリケーション制御），（11 ページ）	アプリケーションまたはアプリケーション特性（タイプ、リスク、ビジネスの関連性、カテゴリ、タグ）	アクセス コントロール ルール SSL ルール アイデンティティ ルール アプリケーション フィルタ インテリジェント アプリケーション バイパス（IAB）

条件	トラフィック制御方法	対応しているルール/設定
URL 条件（URL フィルタリング），（17 ページ）	URL、対応している場合には、URL の特性（カテゴリおよびレピュテーション）	アクセス コントロール ルール SSL ルール
ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御），（25 ページ）	ホストのログイン権限のあるユーザまたはそのユーザのレルム、グループ、または ISE 属性	アクセス コントロール ルール SSL ルール（ISE 属性なし）

ルール条件の仕組み

ルール条件では、各ルールで処理するトラフィックを指定します。各ルールに複数の条件を設定し、トラフィックがルールに一致するにはすべての条件を満たす必要があります。使用可能な条件タイプは、ルール タイプによって異なります。

ルール エディタには、条件タイプごとに独自のタブがあります。一致させるトラフィック特性を選択して条件を作成します。一般に、左側の使用可能な項目のリスト（1 つまたは 2 つ）から基準を選択し、それらの基準を右側の選択済み項目のリスト（1 つまたは 2 つ）に追加します。たとえば、アクセス コントロール ルールの URL 条件では、URL カテゴリとレピュテーション基準を組み合わせて、ブロックする Web サイトのグループを 1 つ作成できます。

条件を作成しやすくするために、レルム、ISE 属性、さまざまなタイプのオブジェクトやオブジェクト グループなど、さまざまなシステム提供の構成やカスタム構成を使用して、トラフィックを照合できます。多くの場合、ルール基準は手動で指定できます。

送信元と宛先の基準

ルールに送信元と宛先の基準（ゾーン、ネットワーク、ポート）が含まれる場合、通常は一方または両方の基準を制約として使用できます。両方を使用する場合、一致するトラフィックの発信元は、指定した送信元のゾーン、ネットワーク、またはポートのいずれかであり、宛先のゾーン、ネットワーク、またはポートのいずれかから送出される必要があります。

条件ごとの項目

最大 50 個の項目を各条件に追加できます。送信元と宛先の基準を含むルールでは、それぞれ最大 50 個使用できます。選択した項目のいずれかに一致するトラフィックが条件に一致します。

単純なルールの仕組み

ルール エディタには、次の一般的な選択肢があります。条件の作成の詳細な手順については、各条件タイプのトピックを参照してください。

- 項目の選択（Choose Item）：項目をクリックするか、そのチェックボックスにマークを付けます。多くの場合、Ctrl または Shift キーを使用して複数の項目を選択するか、右クリックして [すべて選択（Select All）] を選択できます。

- 検索（Search）：検索フィールドに基準を入力します。入力するとリストが更新されます。項目名が検索され、オブジェクトとオブジェクト グループについては、その値が検索されます。リロード（）またはクリア（）をクリックして検索をクリアします。
- 事前定義された項目の追加（Add Predefined Item）：1 つ以上の使用可能な項目を選択し、[追加（Add）]ボタンをクリックするか、ドラッグアンドドロップします。無効な項目（重複、無効な組み合わせなど）は追加できません。
- 手動項目の追加（Add Manual Item）：[選択済み（Selected）]項目リストの下のフィールドをクリックし、有効な値を入力して [追加（Add）] をクリックします。ポートを追加すると、ドロップダウン リストからプロトコルも選択できます。
- オブジェクトの作成（Create Object）：追加アイコン（）をクリックし、作成する条件ですぐに使用できる新しい再利用可能オブジェクトを作成し、オブジェクト マネージャで管理できます。この方法を使用してアプリケーション フィルタをその場で追加した場合、別のユーザ作成フィルタが含まれるフィルタを保存することはできません。
- 削除（Delete）：項目の削除アイコン（）をクリックするか、1 つ以上の項目を選択し、右クリックして [選択項目の削除（Delete Selected）] を選択します。

セキュリティ ゾーンの条件

セキュリティ ゾーンを利用すると、ネットワークをセグメント化し、複数のデバイスでインターフェイスをグループ化して、トラフィック フローを管理および分類する上で助けになります。

ゾーンのルール条件では、トラフィックをその送信元と宛先のセキュリティ ゾーンで制御します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッドまたはASA FirePOWER）でなければならないのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプでなければなりません。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブ インターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

ヒント ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

セキュリティ ゾーン条件を使用したルール

次のルールは、セキュリティ ゾーン条件をサポートします。

- アクセス コントロール
- SSL
- DNS（送信元ゾーンの制約のみ）
- アイデンティティ
- ネットワーク分析

例：セキュリティ ゾーンを使用したアクセス制御

ホストにインターネットへの無制限接続を提供しつつ、それでも着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したいという展開を想定します。

最初に、内部と外部の 2 つのセキュリティ ゾーンを作成します。次に、1 つ以上のデバイスでインターフェイスのペアをこれらのゾーンに割り当てます。この際、1 つのインターフェイスは内部ゾーンの各ペアに割り当て、1 つは外部ゾーンに割り当てます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

（注） 内部（または外部）のすべてのインターフェイスを1つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

次に、宛先ゾーンの条件が内部に設定されているアクセス コントロール ルールを設定します。この単純なルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。一致するトラフィックを侵入やマルウェアについて検査するには、ルール アクションとして [許可（Allow）] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。

ネットワーク条件

ネットワーク ルールの条件では、内部ヘッダーを使用して、送信元と宛先のIPアドレスを基準にトラフィックを制御します。外部ヘッダーを使用するトンネル ルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々のIPアドレスまたはアドレス ブロックを手動で指定することもできます。

（注） 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。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ネットワーク条件での地理位置情報

ルールによっては、送信元または宛先の地理的位置を使用してトラフィックを照合することもできます。ルールのタイプが地理位置情報をサポートするものであれば、ネットワーク条件と地理位置情報条件を混在させることができます。トラフィックのフィルタリングに最新の地理位置情報データが使用されるよう、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

ネットワーク条件を使用したルール

ルール タイプ	地理位置情報による制約のサポート
アクセス コントロール	Yes
SSL	Yes
DNS（送信元ネットワークのみ）	No
ID（Identity）	Yes
ネットワーク分析	No

ネットワーク条件の設定

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/Access Admin/Network Admin

手順

ステップ 1 ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

ステップ 2 [利用可能なネットワーク（Available Networks）] リストから追加する定義済みネットワークを見つけて選択します。
ルールが地理位置情報をサポートしている場合は、ネットワークと地理位置情報の基準を同じルールに混在させることができます。

- [ネットワーク（Networks）] : [ネットワーク（Networks）] サブタブをクリックして、ネットワークを選択します。

- [地理位置情報（Geolocation）]：[地理位置情報（Geolocation）]サブタブをクリックして、地理位置情報オブジェクトを選択します。

ステップ 3 [送信元に追加（Add to Source）]、[元のクライアントに追加（Add to Original Client）]、または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

ステップ 4 手動で指定するネットワークを追加します。送信元または宛先 IP アドレスかアドレスブロックを入力し、[追加（Add）] をクリックします。

（注） 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。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールのネットワーク条件

次の図は、内部ネットワークから発生し、北朝鮮または 93.184.216.119（example.com）のリソースにアクセスしようとする接続をブロックするアクセス コントロール ルールのネットワーク条件を示しています。

この例で、「Private Networks」と呼ばれるネットワーク オブジェクト グループ（図に示されていない IPv4 および IPv6 プライベート ネットワークのネットワーク オブジェクトから構成されます）は、内部ネットワークを表します。また、example.com の IP アドレスを手動で指定し、システムが提供する北朝鮮の地理位置情報オブジェクトを使用して北朝鮮の IP アドレスを表しています。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

VLAN 条件

VLAN ルール条件によって、VLAN タグ付きトラフィックが制御されます。システムでは、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

（注） 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。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

VLAN 条件が含まれたルール

次のルール タイプでは、VLAN 条件がサポートされます。

- アクセス コントロール
- SSL
- DNS
- アイデンティティ
- ネットワーク分析

ポートおよび ICMP コードの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP および UDP トラフィックは、トランスポート層プロトコルに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号 + オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- ポートなし：ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポートプロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。
- SSL ルール：SSL ルールは TCP ポート条件のみをサポートします。
- アイデンティティ ルール：システムは非 TCP トラフィックに対してアクティブ認証を適用できません。アイデンティティ ルールのアクションが [アクティブ認証（Active Authentication）] の場合、あるいは [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（Use active authentication if passive authentication cannot identify user）] オプションをオンにする場合は、TCP ポート制約のみを使用してください。アイデンティティ ルール アクションが [パッシブ認証（Passive Authentication）] または [認証なし（No Authentication）] である場合、非 TCP トラフィックに基づいてポート条件を作成できます。

注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。
アクティブ認証ルールには [アクティブ認証（Active Authentication）] ルール アクションが含まれているか、または [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（Use active authentication if passive authentication cannot identify user）] が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれています。

- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

ポート条件を使用したルール

次のルールは、ポート条件をサポートします。

- アクセス コントロール
- SSL（TCP トラフィックのみをサポート）
- アイデンティティ（アクティブ認証は TCP トラフィックのみをサポート）

ポート条件の設定

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/Access Admin/Network Admin

手順

ステップ 1 ルール エディタで、[ポート（Ports）] タブをクリックします。

ステップ 2 [利用可能なポート（Available Ports）] リストから追加する定義済みポートを見つけて選択します。

ステップ 3 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元ポートまたは宛先ポートを追加します。

- [送信元（Source）]：プロトコルを選択し、0 から 65535 までのポートを 1 つ入力して [追加（Add）] をクリックします。
- [宛先（ICMP 以外）（Destination (non-ICMP)）]：プロトコルを選択または入力します。プロトコルを指定しない場合、または [TCP] か [UDP] を選択した場合は、0 から 65535 までのポートを 1 つ入力します。[追加（Add）] をクリックします。
- [宛先（ICMP）（Destination (ICMP)）]：[プロトコル（Protocol）] ドロップダウン リストから [ICMP] または [IPv6-ICMP] を選択し、表示されるポップアップ ウィンドウでタイプおよび関連するコードを選択します。ICMP タイプとコードの詳細については、Internet Assigned Numbers Authority（IANA）の Web サイトを参照してください。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

アプリケーション条件（アプリケーション制御）

システムは IP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能フィルタを作成できます。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。

アプリケーション フィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニタされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーション条件の設定

次の表に示す設定を行い、アプリケーション制御を実行します。この表には、設定する内容により、アプリケーション制御にどのような制約を設けることができるかも示します。

設定（Configuration）	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ
アクセス コントロール ルール	Yes	Yes	Yes
SSL ルール	Yes	No：SSL プロトコル タグによって、自動的に暗号化アプリケーション トラフィックに制約される	No
IDルール（アクティブ認証からアプリケーションを免除）	Yes	No：ユーザ エージェント除外タグによって、自動的に制約される	No
オブジェクト マネージャ内のユーザ定義のアプリケーション フィルタ	Yes	Yes	No：ユーザ定義のフィルタのネストは不可

設定（Configuration）	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ
インテリジェントアプリケーションバイパス（IAB）	Yes	Yes	Yes

関連トピック

概要：アプリケーション検出

アプリケーション条件とフィルタの設定

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）	Control	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

アプリケーションの条件またはフィルタを作成するには、使用可能なアプリケーションのリストから、トラフィックを制御するアプリケーションを選択します。オプションとして（推奨）、フィルタを使用して使用可能なアプリケーションを抑制します。フィルタと個別に指定されたアプリケーションを同じ条件で使用できます。

はじめる前に

- アクセス コントロール ルールでアプリケーション制御を実行するためには、適応型プロファイルの設定 で説明されているように、アダプティブ プロファイルを有効にする**必要があります**。

手順

ステップ 1 ルール エディタまたは設定エディタを起動します。

- アクセス コントロール、SSL ルール条件：ルール エディタで [アプリケーション（Applications）] タブをクリックします。
- アイデンティティ ルール条件：ルール エディタで [レルムおよび設定（Realms & Settings）] タブをクリックし、アクティブ認証を有効にします。アイデンティティ ルールとレルムの関連付けを参照してください。

- アプリケーション フィルタ：オブジェクト マネージャの [アプリケーション フィルタ（Application Filters）] ページで、アプリケーション フィルタを追加または編集します。フィルタの一意の名前を指定します。
- インテリジェント アプリケーション バイパス（IAB）：アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、IAB の設定を編集して、[バイパス可能なアプリケーションおよびフィルタ（Bypassable Applications and Filters）] をクリックします。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

[使用可能なアプリケーション（Available Applications）] に表示されるアプリケーションを抑制するには、1 つ以上のアプリケーション フィルタを選択するか、個別のアプリケーションを検索します。使用可能なアプリケーションを抑制した後に、フィルタに一致するすべてのアプリケーションを追加したり、個別のアプリケーションを選択および追加したりできます。

ヒント サマリー情報とインターネットの検索リンクを表示するには、アプリケーションの横の情報アイコン（）をクリックします。ロック解除アイコン（）は、システムが復号されたトラフィックでのみ識別できるアプリケーションを示します。

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、ユーザ定義フィルタはできません。

- 同じ特性（リスク、ビジネス関連性など）の複数のフィルタ：アプリケーション トラフィックは 1 つのフィルタのみに一致する必要があります。たとえば、中リスク フィルタと高リスク フィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストにすべての中リスク アプリケーションと高リスク アプリケーションが表示されます。
- 異なるアプリケーション特性のフィルタ：アプリケーション トラフィックは、両方のフィルタ タイプに一致する必要があります。たとえば、高リスク フィルタとビジネスとの関連性が低いフィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストに両方の条件を満たすアプリケーションのみが表示されます。

ステップ 3 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

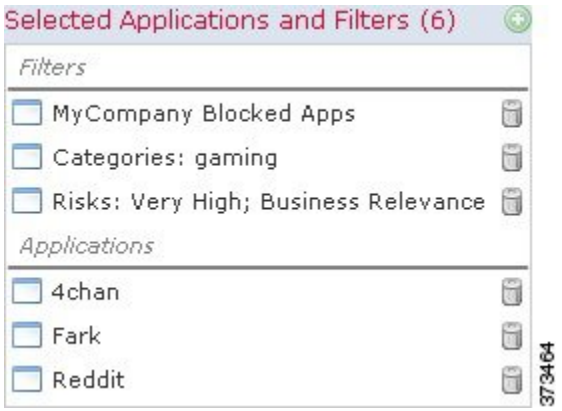
ヒント フィルタとアプリケーションをさらに追加する前に、[フィルタのクリア（Clear Filters）] をクリックして現在の選択をクリアします。

Web インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

ステップ 4 ルールまたは設定を保存するか、編集を続けます。

例：アクセス コントロール ルールのアプリケーション条件

次の図は、MyCompany のユーザ定義アプリケーション フィルタ、リスクが高くビジネスとの関連性が低いすべてのアプリケーション、ゲーム アプリケーション、および個々に選択されたいくつかのアプリケーションをブロックするアクセス コントロール ルールのアプリケーション条件を示しています。



次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *1*：アプリケーションの特性

特性	説明	例
タイプ（Type）	アプリケーション プロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ（Category）	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。

特性	説明	例
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

アプリケーション制御の制限

アプリケーション ディテクタの自動有効化

ディテクタが検出対象のアプリケーションに対して有効でない場合、システムは、そのアプリケーションに対応するシステム提供のすべてのディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

アプリケーション識別の速度

システムは、次が実行されるまで、インテリジェント アプリケーション バイパス（IAB）アプリケーション制御を実行できません。

- モニタ対象の接続がクライアントとサーバの間で確立され、
- システムがセッションでアプリケーションを識別する

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、アクセス コントロール ポリシーのデフォルトの侵入ポリシー（デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）によりインスペクションが実行されます。

暗号化および復号トラフィックのアプリケーション制御

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、POPS、FTPS、TelnetS、IMAPS を含む StartTLS で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションに `SSL Protocol` タグが付けられます。SSL ルールでは、これらのアプリケーションのみを選択できます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。

- 復号トラフィック：システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに `decrypted traffic` タグを割り当てます。

アプリケーションのアクティブ認証の免除

アイデンティティ ポリシーでは、特定のアプリケーションのアクティブ認証を免除し、トラフィックにアクセス コントロールの続行を許可できます。これらのアプリケーションには、`User-Agent Exclusion` タグが付けられます。アイデンティティ ルールでは、これらのアプリケーションのみを選択できます。

ペイロードのないアプリケーション トラフィック パケットの処理

アクセス コントロールを実行している場合、システムは、アプリケーションが識別された接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるアプリケーション トラフィックの処理

アドバタイズメント トラフィックなどの Web サーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype）

システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skype のトラフィックを制御するには、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出してコントロールできるようになります。

コンテンツ制限機能用にサポートされる検索エンジン

システムは、特定の検索エンジンの場合のみ、セーフサーチ フィルタリングをサポートします。システムは、これらの検索エンジンからのアプリケーション トラフィックに `safesearch supported` タグを割り当てます。

関連トピック

デフォルトの侵入ポリシー
アプリケーション検出に関する特殊な考慮事項

URL 条件（URL フィルタリング）

URL 条件は、ネットワークのユーザがアクセスできる Web サイトを制御します。この機能は、*URL* フィルタリングと呼ばれます。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリング ライセンスでは、URL の一般的な分類（カテゴリ）とリスク レベル（レピュテーション）に基づいて Web サイトへのアクセスを制御することができます。

- 手動 URL フィルタリング：任意のライセンスで、個々の URL、URL のグループおよび URL リストとフィードを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム *HTTP* 応答ページを表示できます。インタラクティブ ブロッキングは、警告ページをクリック スルーすることで Web サイトのブロックをバイパスする機会をユーザに与えます。詳細については、HTTP応答ページとインタラクティブ ブロッキングを参照してください。

URL 条件を伴うルール

次の表に、URL条件をサポートするルールと、各ルールタイプがサポートするフィルタリングのタイプを一覧します。

ルール タイプ	カテゴリとレピュテーションのサポートフィルタリングの有無	手動フィルタリングのサポート
アクセス コントロール	Yes	Yes
SSL	Yes	なし。代わりに識別名条件を使用

レピュテーションベースの URL フィルタリング

URL フィルタリング ライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、高リスク（レベル 1）からウェルノウン（レベル 5）の範囲です。

（注） イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。また、Cisco Collective Security Intelligence（CSI）との通信を有効にして、最新の脅威インテリジェンスを取得する必要もあります。

レピュテーションベースの URL フィルタリングの利点

URLカテゴリとレピュテーションによって、URLフィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、乱用薬物カテゴリの高リスク URL をブロックできます。

カテゴリおよびレピュテーション データを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。脅威インテリジェンスは、新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して要求された URL をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザが新しいポリシーを更新したり展開したりするペースを上回って次々と現れては消える可能性があります。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで自動的にブロックできます。
- アクセス コントロール ルールですべてのマルウェア サイトをブロックし、あるブログ ページがマルウェアに感染すると、システムはその URL をブログからマルウェアに再分類して、そのサイトをブロックすることができます。
- アクセス コントロール ルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、システムはそのページのレピュテーションを無害なサイトから高リスクに変更してブロックすることができます。

関連トピック

集合型セキュリティ インテリジェンスの通信設定オプション
Snort® の再起動シナリオ

手動 URL フィルタリング

アクセス コントロール ルール ルールでは、個々の URL、URL のグループ、または URL のリストとフィードを手動でフィルタリングすることで、カテゴリとレピュテーション ベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。

（注） 多数の URL をフィルタリングする場合、個別の、またはグループ化された URL オブジェクトを使用する代わりに、URL リストを使用します。詳細については、セキュリティインテリジェンスのリストとフィードを参照してください。

特殊なライセンスなしでこのタイプの URL フィルタリングを実行することができます。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

たとえば、アクセス コントロールを使用して組織に適していない Web サイトのカテゴリをブロックできます。ただし、カテゴリに適切な Web サイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で許可ルールを作成し、カテゴリのブロック ルールの前に配置できます。

特定のURLを手動でフィルタリングする場合、影響を受ける可能性のある他のトラフィックについて慎重に検討してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の一部に一致すると、 URL が一致したと見なされます。

たとえば example.com へのすべてのトラフィックを許可する場合、ユーザは次の URL を含むサイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

別の例として、ign.com（ゲーム サイト）を明示的にブロックする場合を考えてください。部分文字列マッチングにより ign.com 自体だけでなく verisign.com もブロックされることになり、意図しない動作が生じる可能性があります。

関連トピック

セキュリティ インテリジェンスのリストとフィード

URL 条件の設定

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）
URL フィルタリング（カテゴリ/レピュテーション） 任意（手動）	URL フィルタリング（カテゴリ/レピュテーション） 任意（手動）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

URL 条件を作成するときに、トラフィックを制御する URL カテゴリを選択します。必要に応じて、URL カテゴリをレピュテーションで制約できます。

アクセス コントロール ルールでは、事前定義された URL オブジェクト、URL リストとフィード、および手動のルールごとのURLを使用して個々のURLをフィルタ処理することもできます。これらの URL はレピュテーションで制約できません。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

注意 アクセス コントロールまたはSSLルールの URL またはカテゴリ/レピュテーションの最初の条件を追加するかまたは最後の条件を削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 ルール エディタで、URL 条件のタブをクリックします。

- アクセス コントロールまたは ：[URL（URLs）] タブをクリックします。
- SSL：[カテゴリ（Categoy）] タブをクリックします。

ステップ 2 制御する URL を見つけて選択します。

- カテゴリ：URL の URL カテゴリを選択するか、デフォルトの [任意（Any）] のままにします。アクセス コントロール ルールでは、[カテゴリ（Categoy）] サブタブをクリックしてカテゴリを選択します。
- URL オブジェクト、リスト、およびフィード：定義済みの URL オブジェクトおよび URL リストとフィードを選択します。アクセス コントロール ルールでは、[URL（URLs）] サブタブをクリックして URL を選択します。

ステップ 3 （オプション）レピュテーションを選択して URL カテゴリを制約します。
レピュテーション レベルを選択すると、ルール アクションに応じて、選択したレベルよりも重大または重大でない他のレピュテーションも含められます。ルール アクションを変更すると、URL 条件のレピュテーション レベルが自動的に変更されます。

- [より重大でないレピュテーションを含める（Includes less severe reputations）]：ルールで Web トラフィックを許可または信頼する場合。たとえば、無害なサイト（レベル 4）を許可するようアクセス コントロール ルールを設定した場合、有名（レベル 5）サイトも自動的に許可されます。
- [より重大なレピュテーションを含める（Includes more severe reputations）]：ルールで Web トラフィックを、復号、ブロック、またはモニタする場合。たとえば、疑わしいサイト（レベル 2）をブロックするようアクセス コントロール ルールを設定した場合、高リスク（レベル 1）のサイトも自動的にブロックされます。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）アクセス コントロール ルールでは、URL を入力し、[追加（Add）] をクリックして、手動で指定する URL を追加します。
URL または IP アドレスを入力できます。このフィールドでは、ワイルドカードはサポートされません。

ステップ 6 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールの URL 条件

次の図は、すべてのマルウェア サイト、すべての高リスク サイト、およびすべての有害なソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルールの URL 条件を示し

ています。また、単一サイト example.com（URL オブジェクトによって表されます）もブロックされます。

次の表では、条件を作成する方法を要約します。

ブロックする URL	カテゴリまたはURLオブジェクト	レピュテーション
マルウェアサイト（レピュテーションに関係なく）	マルウェア サイト（Malware Sites）	任意（Any）
高リスクの URL（レベル 1）	任意（Any）	1 - 高リスク（High Risk）
無害（benign）よりも大きいリスクがあるソーシャル ネットワーキング サイト（レベル 1 ～ 3）	ソーシャル ネットワーク（Social Network）	3 - セキュリティ リスクのある無害なサイト（Benign sites with security risks）
example.com	example.com という名前の URL オブジェクト	none

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムは SSL ハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。アクセス コントロール ポリシーで HTTPS URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

また、HTTPS フィルタリングは URL リストもサポートしていません。代わりに、URL オブジェクトとグループを使用する必要があります。

ヒント SSL ポリシーでは、特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。HTTPS トラフィックを復号すると、アクセス コントロール ルールが復号されたセッションを評価できるようになるため、URL フィルタリングが改善します。

暗号化プロトコルによるトラフィックの制御

アクセス コントロール ポリシー内で URL フィルタリングを実行する場合、暗号化プロトコル（HTTP または HTTPS）は無視されます。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックのみに一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

Action: Allow
Application: HTTPS
URL: example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

Action: Block
Application: HTTP
URL: example.com

URL フィルタリングの制限

URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムがセッションで HTTP または HTTPS アプリケーションを識別する。
- システムが要求された URL を識別する（ClientHello メッセージまたはサーバ証明書からの暗号化されたセッションの場合）。

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッショントラフィックに適切なルールアクションを適用します。

アクセス制御の場合、これらの受け渡されたパケットは、デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもなく、アクセス制御ポリシーのデフォルトの侵入ポリシーによりインスペクションが実行されます。

カテゴリまたはレピュテーションが不明な URL

URL のカテゴリまたはレピュテーションが不明な場合、Web サイトの閲覧は、カテゴリまたはレピュテーションベースの URL 条件を持つルールには一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

手動 URL フィルタリング

特定のURLを手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の任意の部分に一致する場合、URL は一致するとみなされます。

暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- URL リストを使用しません。代わりに、URL オブジェクトとグループを使用する必要があります。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化されたまたは復号された接続の場合は HTTP 応答ページを表示しません。HTTP 応答ページの制限を参照してください。

URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

選択したデバイス モデルのメモリ制限

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なるURLカテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親URLのデータが使用されます。具体的な例として、システムはgoogle.comカテゴリとレピュテーションを使用して mail.google.com を評価します。

メモリが少ないデバイスには、7100 ファミリと次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。NGIPSv で、カテゴリおよびレピュテーション ベースの URL フィルタリングを実行するための正しいメモリ量を割り当てる方法ついて、詳しくは *Firepower System Virtual Installation Guide*を参照してください。

関連トピック

デフォルトの侵入ポリシー

ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）

Firepowerシステムによって収集された権限のあるユーザアイデンティティデータを使用してユーザ制御を実行することができます。

アイデンティティ ソースはユーザがログインまたはログアウトする際、または Microsoft Active Directory（AD）またはLDAPのクレデンシャルを使用して認証する際にユーザをモニタします。次に、この収集されたアイデンティティ データを使用して、モニタ対象ホストに関連付けられているログインしている権限のあるユーザに基づいてトラフィックを処理するルールを設定できます。ユーザは、そのユーザがログオフする（アイデンティティ ソースによって報告される）か、レルムがセッションをタイムアウトするか、システムのデータベースからそのユーザ データが削除されるまで、ホストに関連付けられたままになります。

Firepower システムのご使用のバージョンでサポートされる権限のあるユーザ アイデンティティ ソースについては、ユーザ アイデンティティ ソースについてを参照してください。

ユーザ制御を実行するために、次のルール条件を使用できます。

- ユーザ条件およびレルム条件：ホストのログインしている権限のあるユーザに基づいてトラフィックを照合します。トラフィックは、レルム、個々のユーザ、またはそれらのユーザが属しているグループに基づいて制御できます。
- ISE 属性条件：ユーザの、ISE が割り当てたセキュリティ グループ タグ（SGT）、デバイス タイプ（エンドポイント プロファイルとも呼ばれる）、またはロケーション IP（エンドポイント ロケーションとも呼ばれる）に基づいてトラフィックを照合します。ISE をアイデンティティ ソースとして設定する必要があります。

ユーザ条件を持つルール

ルール タイプ	ユーザ条件およびレルム条件のサポート	ISE 属性条件のサポート
アクセス コントロール	Yes	Yes
SSL	Yes	No

関連トピック

ユーザ エージェントのアイデンティティ ソース
ISE アイデンティティ ソース
キャプティブ ポータルのアイデンティティ ソース

ユーザ制御の前提条件

アイデンティティ ソース/認証方式の設定

実行する認証タイプのアイデンティティ ソースを設定します。詳細については、ユーザアイデンティティ ソースについてを参照してください。

ユーザ エージェントまたはISEデバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルム、ユーザ、またはユーザ グループの条件のルールが、一致することが想定されているトラフィックと一致しなくなる可能性があります。

レルムの設定

監視対象の各 AD または LDAP サーバ（ISE またはユーザ エージェント サーバを含む）のレルムを設定し、ユーザのダウンロードを実行します。詳細については、レルムの作成を参照してください。

レルムを設定するときには、アクティビティを監視するユーザおよびユーザ・グループを指定します。ユーザ グループを含めると、自動的に、すべてのセカンダリ グループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、セカンダリ グループをルール条件として使用する場合は、セカンダリ グループをレルム構成に明示的に含める必要があります。

レルムごとに、ユーザデータの自動ダウンロードを有効にすると、ユーザおよびユーザ グループの信頼できるデータを更新することができます。

アイデンティティ ポリシーの作成

レルムを認証方式に関連付けるアイデンティティ ポリシーを作成し、そのポリシーをアクセス制御に関連付けます。詳細については、アイデンティティ ポリシーの作成を参照してください。

デバイスのユーザ制御（アクセス制御、SSL）を実行するポリシーは、アイデンティティ ポリシーを共有します。そのアイデンティティ ポリシーによって、それらのデバイス上のトラフィックに影響するルールで使用できるレルム、ユーザ、およびグループが決まります。

ユーザおよびレルム条件の設定

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）	Control	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

レルム、またはそのレルム内のユーザとユーザ グループでルールを制約できます。

はじめる前に

- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）, （25 ページ）で説明されているユーザ制御の前提条件を満たしてください。

手順

ステップ 1 ルール エディタで、[ユーザ（Users）] タブをクリックします。

ステップ 2 （オプション）[利用可能なレルム（Available Realms）] リストから使用するレルムを見つけて選択します。

ステップ 3 （オプション）[有効なユーザ（Available Users）] リストからユーザとグループを選択して、ルールをさらに制約します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

ISE 属性条件の設定

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）	Control	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

はじめる前に

- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御），（25 ページ）に記載されているユーザ制御の前提条件を満たします。

手順

ステップ 1 ルール エディタで、[ISE 属性（ISE Attributes）] タブをクリックします。

ステップ 2 [使用可能な属性（Available Attributes）] リストから、使用する ISE 属性を見つけて選択します。

- [セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）]
- [デバイス タイプ（Device Type）]（エンドポイント プロファイルとも呼ばれます）
- [ロケーション IP（Location IP）]（エンドポイント ロケーションとも呼ばれます）

ステップ 3 [使用可能なメタデータ（Available Metadata）] リストから属性メタデータを選択して、さらにルールを制約します。または、デフォルトの [すべて（any）] のままにします:。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）[ロケーション IP アドレスの追加（Add a Location IP Address）] フィールドで、IP アドレスによりルールを制約し、[追加（Add）] をクリックします。
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。

ステップ 6 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

ユーザ制御のトラブルシューティング

ユーザ ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。その他の関連するトラブルシューティング情報については、以下を参照してください。

- ユーザ エージェント アイデンティティ ソースのトラブルシューティング
- ISE アイデンティティ ソースのトラブルシューティング
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング
- レルムとユーザのダウンロードのトラブルシューティング

レルム、ユーザ、またはユーザ グループを対象とするルールがトラフィックと一致しない

ユーザ エージェントまたは ISE デバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがユーザ レコードをドロップすることがあります。その結果、ユーザ条件のルールが、一致することが想定されているトラフィックと一致しない可能性があります。

ユーザ グループまたはユーザ グループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

ユーザ グループ条件を含むルールを設定する場合は、LDAP または Active Directory サーバでユーザ グループを設定している必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザ グループ制御を実行できません。

セカンダリ グループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外するユーザ グループ条件を含むルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが Firepower Management Center に報告され、ユーザ条件を含むルールでの使用に適するようにカスタマイズする必要があります。

ルールが、初めて表示されたユーザと一致しない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバからそれらのユーザに関する情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するルールによって**処理されません**。代わりに、ユーザ セッションが、一致する次のルール（または該当する場合はポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザ グループのメンバーであるユーザが、ユーザ グループ条件を含むルールに一致しない。
- ユーザ データの取得に使用されたサーバが Active Directory サーバである場合、ユーザ エージェントまたは ISE デバイスによって報告されたユーザがルールと一致しない。

これにより、システムがユーザデータをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

ルールがすべての ISE ユーザと一致しない

これは想定されている動作です。Active Directory ドメイン コントローラで認証された ISE ユーザに対してユーザ制御を実行することができます。LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。

ルールの検索

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/Access Admin/Network Admin

多くのポリシーでは、ルールとルール内の検索が可能です。システムは、入力内容をルールの名前および条件値と照合します。これには、オブジェクトとオブジェクト グループが含まれます。

セキュリティ インテリジェンスまたは URL のリストまたはフィードに含まれる値は検索できません。

手順

ステップ 1 ポリシー エディタで、[ルール（Rules）] タブをクリックします。

ステップ 2 [ルールの検索（Search Rules）] プロンプトをクリックし、検索文字列のすべてまたは一部を入力してから Enter キーを押します。
照合ルールごとに、一致する値のカラムが強調表示されます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

ステップ 3 目的のルールを見つけます。
照合ルールの間を移動する場合は、次の一致アイコン（ ）または前の一致アイコン（ ）をクリックします。

次の作業

- 新しい検索を開始する前に、クリアアイコン（ ）をクリックして、検索と強調表示をクリアします。

デバイス別のフィルタリング ルール

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）	機能に応じて異なる	任意（Any）	Admin/Access Admin/Network Admin

一部のポリシー エディタでは、該当デバイスによってルールの表示をフィルタ処理することができます。

システムは、ルールがそのデバイスに影響するかどうかを判断するために、ルールのインターフェイス制約を使用します。インターフェイス（セキュリティゾーン条件）でルールを制約すると、インターフェイスが置かれている場所のデバイスがそのルールの影響を受けます。インターフェイス制約のないルールは、すべてのインターフェイスに適用されるので、すべてのデバイスに適用されることになります。

手順

ステップ 1 ポリシー エディタで、[ルール（Rules）] タブをクリックし、[デバイスでフィルタ処理（Filter by Device）] をクリックします。
ターゲット デバイスとデバイス グループのリストが表示されます。

ステップ 2 1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。または、[すべて（All）] をオンにしてリセットし、すべてのルールを表示します。

ヒント ポインタをルール基準に合わせると、その値が表示されます。基準がデバイス特有のオーバーライドを持つオブジェクトを表し、そのデバイスだけでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。基準がドメイン特有のオーバーライドを持つオブジェクトを表し、そのドメインのデバイスでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。

ステップ 3 [OK] をクリックします。

関連トピック

アクセス コントロール ルールの作成および編集

ルールとその他のポリシーの警告

ポリシーおよびルール エディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。

ヒント 警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 *2*：ポリシーのエラー アイコン

アイコン	説明	例
 error	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーションベースのURLフィルタリングを実行するルールは、URLフィルタリング ライセンスのないデバイスをターゲットにする時点まで有効です。その時点で、ルールの横にエラーアイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、URLフィルタリングライセンスを有効にする必要があります。
 警告	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクトグループ、一致するアプリケーションがないアプリケーションフィルタ、除外されたLDAPユーザ、無効なポートなどを使用した条件が含まれます。 一方、警告アイコンがライセンスエラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。
 情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの展開が阻止されることはありません。	アプリケーション制御およびURLフィルタリングが適用されている場合、システムは接続でアプリケーション トラフィックまたはWebトラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより接続を確立することができ、アプリケーションとHTTP要求を識別できるようになります。

関連トピック

アプリケーション制御の制限, （16 ページ）
URL フィルタリングの制限, （23 ページ）

ルールのパフォーマンスに関するガイドライン

Firepowerシステムでは、さまざまなポリシーに含まれるルールが、ネットワーク トラフィックをきめ細かく制御します。ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。それぞれの組織と導入に固有のポリシーとルール セットがありますが、ニーズに対処しながらもパフォーマンスを最適化するために従うべき一般的なガイドラインがいくつかあります。

パフォーマンスの最適化は、リソースを大量に消費する分析を実行する場合は特に重要です。複雑なポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。設定の変更を展開すると、システムはすべてのルールをまとめて評価し、ターゲット デバイスでネットワーク トラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲット デバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに展開することはできません。

（注） 常に、ルールを組織のニーズに適した順序に配置する必要があります。すべてのトラフィックに適用する必要がある最優先順位のルールをポリシーの先頭近くに配置します。ただし、ルールに優先順位を付けなければ、アプリケーション条件またはURL 条件を設定したルールが一致する可能性が高くなります。これは、システムは接続においてアプリケーション トラフィックまたはWeb トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあるためです。これにより接続を確立することができ、アプリケーションとHTTP 要求を識別できるようになります。

関連トピック

アプリケーション制御の制限, （16 ページ）
URL フィルタリングの制限, （23 ページ）

ルールの簡素化および絞り込みのガイドライン

簡素化：設定しすぎない

処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。

個々のルール条件を最小化します。できる限り少ない個々の要素をルールの条件に使用します。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御およびURLフィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAP ユーザ グループを使用します。

要素をオブジェクトに組み合わせても、パフォーマンスは向上**しません**。たとえば、50個のIPアドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリット

はなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

絞り込み：特にインターフェイスによってリソース消費ルールを絞り込んで制約する

できる限り、ルールの条件を使用してリソース消費ルールが処理するトラフィックを絞り込んで定義します。絞り込まれたルールは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。以下は、リソース消費ルールの例です。

- トラフィックを復号する SSL ルール：復号だけでなく、復号されたトラフィックの更なる分析にもリソースが必要です。絞り込みを細かくし、また可能な場合は、暗号化トラフィックをブロックするか、復号しないようにします。
- ディープ インスペクションを呼び出すアクセス コントロール ルール：特に複数のカスタム侵入ポリシーと変数セットを使用している場合、侵入ファイルやマルウェアのインスペクションにはリソースが必要です。ディープインスペクションは必要な場所でのみ呼び出されることを確認してください。

最大のパフォーマンスによるメリットを得るため、インターフェイスによってルールを制約します。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

ルールの順序指定のガイドライン

ルールのプリエンプション

ルールのプリエンプションが発生するのは、評価する順番が前のルールがトラフィックと一致するために、その後のルールが全くトラフィックと一致しない場合です。ルールの条件により、そのルールが他のルールをプリエンプション処理するかどうかが決まります。次の例では、最初のルールが管理トラフィックを許可するため、2 番目のルールがそのトラフィックをブロックできません。

アクセス コントロール ルール 1：管理ユーザを許可
アクセス コントロール ルール 2：管理ユーザをブロック

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初の SSL ルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールをプリエンプション処理します。

SSL ルール 1：VLAN 22 ～ 33 を復号しない
SSL ルール 2：VLAN 27 をブロック

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

アクセス コントロール ルール 1：送信元ネットワーク 10.4.0.0/16 を許可
アクセス コントロール ルール 2：送信元ネットワーク 10.4.0.0/16、VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールがプリエンプション処理されます。

アクセス コントロール ルール 1：VLAN 1 URL www.example.com を許可
アクセス コントロール ルール 2：VLAN 1 URL www.example.com を許可

条件が 1 つでも異なる場合は、後続のルールがプリエンプション処理されることはありません。

アクセス コントロール ルール 1：VLAN 1 URL www.example.com を許可
アクセス コントロール ルール 2：VLAN 2 URL www.example.com を許可

例：プリエンプションを避けるための SSL ルールの順序付け

ここで1つのシナリオとして、信頼できるCA（GoodCA）が悪意のあるエンティティ（BadCA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックは SSL ポリシーを使用してブロックしたいものの、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。CA証明書とすべての中間CA証明書をアップロードした後、ルールを以下の順序で設定した SSL ポリシーを構成します。

SSL ルール 1：発行元 CN=www.badca.com をブロック
SSL ルール 2：発行元 CN=www.goodca.com を復号しない

上記のルールを逆の順序にすると、不正な CA で信頼されたトラフィックを含め、正当な CA で信頼されたすべてのトラフィックが最初に一致することになります。どのトラフィックも後続の不正な CA ルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

ルールのアクションとルールの順序

ルールのアクションによって、一致したトラフィックの処理方法が決まります。パフォーマンスを向上させるには、リソースを集約的に使用するルールを実行する前に、トラフィックの追加処理を実行または保証しないルールを配置してください。これにより、システムはさらに検査する必要のあるトラフィックだけを転送できます。

以下の例は、一連のルールがすべて同等に重要であり、プリエンプションが問題にならない場合に、さまざまなポリシーでルールを順序付ける方法を示しています。

最適な順序：SSL ルール

復号にはリソースが必要になるだけでなく、復号後のトラフィックの分析も必要になります。したがって、トラフィックを復号する SSL ルールを最後に配置します。

1 [モニタ（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。

2 [ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックをブロックするルール。

3 [復号しない（Do not decrypt）]：暗号化トラフィックを復号しないまま、暗号化セッションをアクセス コントロール ルールに渡すルール。これらのセッションのペイロードにディープ インスペクションは適用されません。

4 [復号 - 既知のキー（Decrypt - Known Key）]：既知の秘密キーを使用して着信トラフィックを復号するルール。

5 [復号 - 再署名（Decrypt - Resign）]：サーバ証明書に再署名することによって発信トラフィックを復号するルール。

最適な順序：アクセス コントロール ルール

複数のカスタム侵入ポリシーと変数セットを使用している場合は特に、侵入、ファイル、マルウェアのインスペクションにリソースが必要です。したがって、ディープ インスペクションを呼び出すアクセス コントロール ルールを最後に配置します。

1 [モニタ（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。

2 [信頼（Trust）]、[ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックを処理するルール。信頼できるトラフィックは、アイデンティティ ポリシーが課す認証要件の対象となることに注意してください。

3 [許可（Allow）]、[インタラクティブブロック（ディープインスペクションなし）（Interactive Block (no deep inspection)）]：それ以上のインスペクションを行わずにトラフィックのディスカバリを許可するルール。許可されるトラフィックは、アイデンティティポリシーが課す認証要件の対象となることに注意してください。

4 [許可（Allow）]、[インタラクティブブロック（ディープインスペクションあり）（Interactive Block (deep inspection)）]：禁止されているファイル、マルウェア、エクスプロイトのディープインスペクションを実行するファイルポリシーまたは侵入ポリシーに関連付けられているルール。

コンテンツ規制ルールの順序

SSL とアクセス コントロール ポリシーの両方でルールのプリエンプションを避けるため、YouTube 規制を制御するルールは、セーフサーチ規制を制御するルールの上に配置します。

アクセス コントロール ルールに対してセーフサーチを有効にする場合、システムは検索エンジンのカテゴリを [選択したアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。このアプリケーション カテゴリには YouTube が含まれます。そのため、YouTube トラフィックは、評価の優先順位が上のルールで YouTube EDU が有効にされていない限り、セーフサーチ ルールに一致します。

同様のルールのプリエンプションは、セーフサーチ サポート フィルタを持つ SSL ルールを、評価順序内で特定の YouTube アプリケーション条件を持つ SSL ルールよりも高い順序に配置した場合に生じます。

SSL ルールの順序

証明書がピニングされたサイトからのトラフィックの許可

証明書のピニングを行うと、SSLセッションが確立される前に、サーバの公開キー証明書が、サーバにすでに関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。[復号 - 再署名（Decrypt - Resign）] アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザがすでにその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアントブラウザが、証明書ピニングを使用するサイト windowsupdate.microsoft.com に接続されており、そのトラフィックと一致する SSL ルールを [復号 - 再署名（Decrypt - Resign）] アクションを使用して設定すると、システムはサーバ証明書に再署名してから、クライアント サーバに渡します。この変更されたサーバ証明書は、ブラウザでピニングした windowsupdate.microsoft.com の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての [復号 - 再署名（Decrypt - Resign）] ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。また、接続が成功したか失敗したかに関わらず、ログに記録された接続イベントから証明書を表示できます。

侵入ポリシーの急増を回避するためのガイドライン

アクセス コントロール ポリシーでは、1 つの侵入ポリシーを各許可ルール、インタラクティブ ブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。

ただし、ターゲット デバイスでサポートされるアクセス コントロール ルールや侵入ポリシーには最大数があります。この最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、さまざまな要因によって異なります。

デバイスでサポートされる最大を超えるとアクセス コントロール ポリシーは展開できず、再評価する必要があります。いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーと変数セットのペアを関連付けることができます。一部のデバイスでは、すべての侵入ポリシーに関して 1 つの変数セットだけを使用できる場合や、デバイス全体でただ 1 つの侵入ポリシー/変数セット ペアだけを使用できる場合があります。