# 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。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合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。 別の例としては、QoS ルールの場合、どの QoS ルールでもトラフィックのレート制限という同じ動作をするため、明示的なアクションはありません。
- 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（追跡とログ記録を行うように設計された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。 別の例としては、QoS ルールにはロギングの設定は含まれていません。これは、レート制限されているというだけの理由で接続をロギングすることはできないためです。
- 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
- トンネルとプレフィルタ ルール： トンネルとプレフィルタ ルールのコンポーネント
- SSL ルール： TLS/SSL ルールの作成と変更
- 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
- QoS ルール： QoS 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
- ファイルおよびマルウェア 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
- NAT ルール（Firepower Threat Defense）：Firepower Threat Defense 用のネットワーク アドレス変換（NAT）
- 8000 シリーズ 高速パス 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 |
|---|---|---|
| インターフェイス条件 （6 ページ） | 送信元インターフェイスと宛先インターフェイス、対応している場合にはトンネル ゾーン | アクセス コントロール ルール<br>トンネル ルール<br>プレフィルタ ルール<br>SSL ルール<br>DNS ルール<br>アイデンティティ ルール<br>ネットワーク分析ルール<br>QoS ルール |
| ネットワーク条件 （9 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<br>プレフィルタ ルール<br>SSL ルール<br>DNS ルール<br>アイデンティティ ルール<br>ネットワーク分析ルール<br>QoS ルール |

| 条件 | トラフィック制御方法 | 対応しているルール/設定 |
|---|---|---|
| トンネル エンドポイント条件（12 ページ） | プレーン テキスト用、送信元のトンネル エンドポイントと宛先のトンネル エンドポイント、パススルー トンネル | トンネル ルール |
| VLAN 条件 （14 ページ） | VLAN タグ | アクセス コントロール ルール<br>トンネル ルール<br>プレフィルタ ルール<br>SSL ルール<br>DNS ルール<br>アイデンティティ ルール<br>ネットワーク分析ルール |
| ポートおよび ICMP コードの条件 （15 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<br>プレフィルタ ルール<br>SSL ルール<br>アイデンティティ ルール<br>QoS ルール |
| カプセル化の条件 （17 ページ） | カプセル化プロトコル（非暗号化） | トンネル ルール |
| アプリケーション条件（アプリケーション制御） （17 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<br>SSL ルール<br>アイデンティティ ルール<br>QoS ルール<br>アプリケーション フィルタ<br>インテリジェント アプリケーション バイパス（IAB） |
| URL 条件（URL フィルタリング） （27 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<br>SSL ルール<br>QoS ルール |

| 条件 | トラフィック制御方法 | 対応しているルール/設定 |
|---|---|---|
| ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （28 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<br>SSL ルール（ISE 属性なし）<br>QoS ルール |
| カスタム SGT 条件 （33 ページ） | カスタム セキュリティ グループ タグ（SGT） | アクセス コントロール ルール<br>QoS ルール |

# 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 ページがあります。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。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

**注意** アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

### 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。

# インターフェイス条件

インターフェイスルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイスオブジェクトを使用してインターフェイス条件を構築できます。インターフェイスオブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィックフローを制御し、分類しやすくします。インターフェイス オブジェクト：インターフェイスグループとセキュリティゾーンを参照してください。

**ヒント** インターフェイスによってルールを制約するのは、システムパフォーマンスを改善するための最適な方法の1つです。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。

インターフェイスオブジェクト内のすべてのインターフェイスが同じタイプ（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）である必要があるのと同様に、インターフェイス条件で使用されているすべてのインターフェイスオブジェクトは同じタイプである必要があります。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、パッシブ展開では宛先インターフェイスでルールを制約することはできません。

### トンネルゾーンとセキュリティ ゾーン

一部の設定では、セキュリティゾーンの代わりにトンネルゾーンを使用してインターフェイス条件を制約できます。トンネルゾーンではプレフィルタを使用して、カプセル化された接続の特定のタイプに合わせて後続のトラフィック処理を調整できます。

**（注）** トンネルゾーンの制約がサポートされる設定の場合、再区分された接続、つまり割り当てられたトンネルゾーンを持つ接続はセキュリティゾーンの制約と一致**しません**。詳細については、トンネル ゾーンおよびプレフィルタリングを参照してください。

### インターフェイス条件を持つルール

| ルール タイプ | セキュリティ ゾーンのサポート | トンネルゾーンのサポート | インターフェイス グループのサポート |
|---|---|---|---|
| アクセス コントロール | はい | はい | いいえ（No） |
| トンネルとプレフィルタ | Yes | 該当なし。プレフィルタポリシー内でトンネルゾーンを割り当てます | 可 |
| SSL | はい | いいえ | いいえ |
| DNS（送信元のみ） | はい | いいえ | いいえ |
| ID（Identity） | はい | いいえ | いいえ |

| ルール タイプ | セキュリティ ゾーンのサポート | トンネルゾーンのサポート | インターフェイス グループのサポート |
|---|---|---|---|
| ネットワーク分析 | はい | いいえ | いいえ |
| QoS（ルーテッドのみ、必須） | はい | いいえ | はい |

### 例：セキュリティ ゾーンを使用したアクセス制御

たとえば、ホストがインターネットに無制限でアクセスできるような導入にする一方、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します。

それにはまず、内部ゾーンと外部ゾーンという 2 つのセキュリティ ゾーンを作成します。次に、これらのゾーンに 1 つ以上のデバイス上のインターフェイス ペアを割り当て、各ペアの一方のインターフェイスを内部ゾーンに割り当て、もう一方のインターフェイスを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、宛先ゾーン条件を内部に設定したアクセス コントロール ルールを構成します。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でデバイスから出力さ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。

## インターフェイス条件の設定

| 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | いずれか（Any） | いずれか（Any） | Admin/Access Admin/Network Admin |

### 始める前に

- （アクセス コントロールのみ）セキュリティ ゾーンではなくトンネル ゾーンによってトラフィックを制約する場合は、関連付けられたプレフィルタ ポリシーがそれらのゾーンを割り当てるようにします。アクセス制御への他のポリシーの関連付けを参照してください。

**ステップ 1** ルール エディタで、インターフェイス条件のタブをクリックします。

- インターフェイス グループおよびセキュリティ ゾーン（トンネル、プレフィルタ、QoS）：[インターフェイス オブジェクト（Interface Objects）] タブをクリックします。
- セキュリティ ゾーン（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）：[ゾーン（Zones）] タブをクリックします。
- トンネルゾーン（アクセス コントロール）：[ゾーン（Zones）] タブをクリックします。

**ステップ 2** [使用可能なインターフェイス オブジェクト（Available Interface Objects）] または [利用可能なゾーン（Available Zones）] リストから追加するインターフェイスを見つけて選択します。

（アクセス コントロールのみ）再ゾーン分割されたトンネルでの接続を一致させるには、セキュリティ ゾーンではなくトンネル ゾーンを選択します。同じルールでトンネル ゾーンとセキュリティ ゾーンを使用することはできません。詳細については、トンネル ゾーンおよびプレフィルタリングを参照してください。

**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** ルールを保存するか、編集を続けます。

### 次のタスク

- （アクセス コントロールのみ）プレフィルタ中にトンネルを再ゾーン分割した場合、完全なカバレッジを確保する必要がある場合は追加のルールを設定します。再ゾーン分割されたトンネルでの接続は、セキュリティ ゾーン制約があるルールに一致**しません**。詳細については、「トンネル ゾーンの使用」を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。

# 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。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

### 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。

### ネットワーク条件での元のクライアント（プロキシ トラフィックのフィルタリング）

一部のルールでは、発信元クライアントに基づいてプロキシ トラフィックを処理できます。送信元ネットワーク条件を使用してプロキシ サーバを指定し、次に元のクライアント制約を追加して元のクライアント IP アドレスを指定します。システムはパケットの X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義 HTTP ヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、さらに元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアント アドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の 3 つのアクセス コントロール ルールを作成します。

アクセス コントロール ルール 1：特定の IP アドレス（209.165.201.1）からの非プロキシ トラフィックをブロックします。

送信元ネットワーク：209.165.201.1
元のネットワーク クライアント：none または any
アクション：ブロック

アクセス コントロール ルール 2：同じ IP アドレスからのプロキシ トラフィックを許可します。ただし、そのトラフィックのプロキシ サーバが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限ります。

送信元ネットワーク：209.165.200.225 および 209.165.200.238
元のクライアント ネットワーク：209.165.201.1
アクション：許可

アクセス コントロール ルール 3：同じ IP アドレスからのプロキシ トラフィックを、それが他のプロキシ サーバを使用する場合はブロックします。

[Source Networks]：any
元のクライアント ネットワーク：209.165.201.1
アクション：ブロック

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 | 元のクライアントによる制約のサポート |
|---|---|---|
| アクセス コントロール | はい | はい |
| プレフィルタ | いいえ | いいえ |
| SSL | はい | いいえ（No） |
| DNS（送信元ネットワークのみ） | いいえ | いいえ |
| ID（Identity） | はい | いいえ（No） |
| ネットワーク分析 | いいえ | いいえ |
| QoS | はい | はい |

## 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | いずれか（Any） | いずれか（Any） | Admin/Access Admin/Network Admin |

**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** （オプション）ルールが元のクライアント制約をサポートしている場合は、[送信元ネットワーク（Source Networks）] で、プロキシされたトラフィックを元のクライアントに基づいて処理するようにルールを設定します。

- [送信元/プロキシ（Source/Proxy）] : [送信元（Source）] サブタブをクリックして、プロキシ サーバを指定します。

- [元のクライアント（Original Client）]：[元のクライアント（Original Client）] サブタブをクリックして、ネットワークを元のクライアント制約として追加します。プロキシ接続では、元のクライアントの IP アドレスは、ルールに一致するネットワークの 1 つと一致する必要があります。

**ステップ 4** [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。

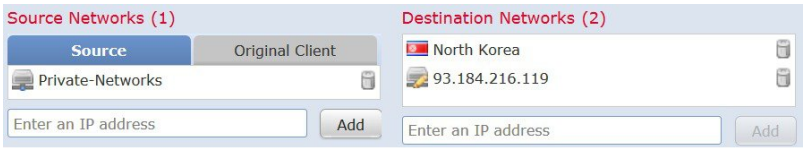
**ステップ 5** 手動で指定するネットワークを追加します。送信元、元のクライアント、または宛先IPアドレスかアドレス ブロックを入力し、[追加（Add）] をクリックします。

（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 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。

### 次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

# トンネル エンドポイント条件

トンネル エンドポイント条件は、トンネル ルールに固有のものです。この条件は、他のルール タイプのネットワーク条件と似ています。

トンネルエンドポイント条件は、特定のタイプのプレーンテキスト、パススルートンネル（カプセル化の条件 （17 ページ）を参照）を制御します。この制御は、それらの送信元と宛先の IP アドレスによって、外側のカプセル化ヘッダーを使用して行います。これらは、トンネル

エンドポイントの IP アドレス、つまり、トンネルのいずれかの側のネットワーク デバイスのルーテッド インターフェイスです。

トンネル ルールはデフォルトでは双方向で、送信元エンドポイントのいずれかと宛先エンドポイントのいずれかとの間の一致するすべてのトンネルを処理します。ただし、送信元から宛先へのトラフィックのみに一致する単方向トンネル ルールを設定できます。トンネルとプレフィルタ ルールのコンポーネントを参照してください。

事前定義済みのネットワーク オブジェクトを使用してトンネル エンドポイント条件を作成したり、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したりできます。

（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。

## トンネル エンドポイント条件の設定

| 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | 該当なし | Firepower Threat Defense | いずれか（Any） | Admin/Access Admin/Network Admin |

**ステップ 1** ルール エディタで、[トンネル エンドポイント（Tunnel Endpoints）] タブをクリックします。

**ステップ 2** [利用可能なトンネル エンドポイント（Available Tunnel Endpoints）] 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。

トンネル エンドポイントは、トンネルの両側にあるネットワーク デバイスのルーテッド インターフェイスの IP アドレスであるため、ネットワーク オブジェクトを使用してトンネル エンドポイント条件を作成できます。

**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。

トンネル ルールはデフォルトでは双方向であるため、2 つのエンドポイント間のすべてのトラフィックを処理できます。ただし、送信元からのトンネルのみを照合するよう選択した場合、トンネル ルールは、送信元から宛先へのトラフィックのみに一致します。

**ステップ 4** 手動で指定するエンドポイントを追加します。送信元か宛先の IP アドレス、またはアドレス 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。

### 次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

# VLAN 条件

VLAN ルール条件によって、QinQ（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、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。

最大 50 個の VLAN 条件を指定できます。

（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 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
- トンネルとプレフィルタ（最も外側の VLAN タグを使用）
- SSL
- DNS
- ID（Identity）
- 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。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

### 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：クラシック デバイスの場合、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。Firepower Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。
- 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。

- ⚠

**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際に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、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は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 **[パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用する（Use active authentication if passive or VPN identity cannot be established）]** 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
- プレフィルタ
- 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）
- QoS

## 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | いずれか（Any） | いずれか（Any） | Admin/Access Admin/Network Admin |

**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。

**次のタスク**

- 設定変更を展開します。設定変更の展開を参照してください。

# カプセル化の条件

カプセル化の条件は、トンネル ルールに固有です。

この条件では、カプセル化プロトコルによって特定のタイプのプレーンテキスト、パススルートンネルを制御します。ルールを保存する前に、一致するプロトコルを 1 つ以上選択する必要があります。次のオプションを選択できます。

- GRE（47）
- IP-in-IP（4）
- IPv6-in-IP（41）
- Teredo（UDP（17）/3455）

# 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。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本を参照してください。

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。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーション制御の一部として、コンテンツ規制を適用するアクセス コントロール ルール（セーフ サーチや YouTube EDU など）を使用することもできます。

**注意** アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

### 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 | コンテンツ規制 |
|---|---|---|---|---|
| アクセス コントロール ルール | はい | はい | はい | はい |
| 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 | いいえ | いいえ |
| 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 | いいえ | いいえ |
| QoS ルール | はい | はい | はい | いいえ（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 | はい | はい | No：ユーザ定義のフィルタのネストは不可 | No |
| インテリジェント アプリケーション バイパス（IAB） | はい | はい | はい | いいえ（No） |

**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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| 任意 | Control | いずれか（Any） | いずれか（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。

### 始める前に

- 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（デフォルト状態）にする**必要があります**。

**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、QoS 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 ルールの作成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** （オプション）セーフ サーチ（）または YouTube EDU（）のグレー表示のアイコンおよび設定関連のオプションをクリックして、アクセス コントロール ルールのコンテンツ制限機能を有効にします。

その他の設定要件については、アクセス コントロール ルールを使用したコンテンツ制限の実施を参照してください。

たいていの場合、コンテンツ制限を有効にすると、条件の [Selected Applications and Filters] リストに適切な値が入力されます。コンテンツ制限を有効にするときに、コンテンツ制限に関係するアプリケーションまたはフィルタがすでにリスト内に存在している場合には、システムはリストに自動的に値を入力することはしません。

アプリケーションを絞り込んで選択内容をフィルタする手順を続行するか、またはスキップしてルールの保存に進みます。

**ステップ 3** [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。

**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 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。

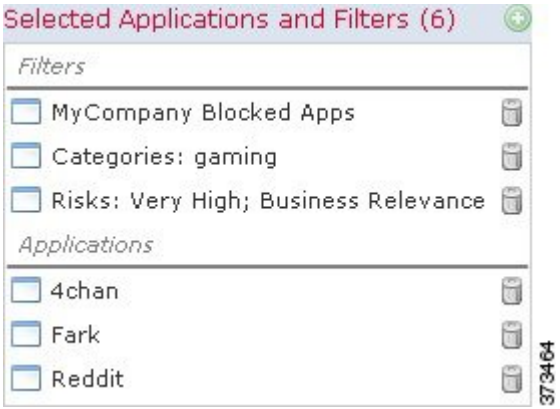
**ヒント** フィルタとアプリケーションをさらに追加する前に、[フィルタのクリア（Clear Filters）] をクリックして現在の選択をクリアします。

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 5** 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。




### 次のタスク

- 設定変更を展開します。設定変更の展開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。<br>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。<br>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。<br>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。<br>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 | 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。 |
| 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（0 を含む）のタグを付けることができます。 | 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ガイドラインと制限事項

### アダプティブ プロファイルが有効になっていることの確認

アダプティブ プロファイルが無効な場合（デフォルト状態）、アクセス制御ルールは、アプリケーション制御を実行できません。

### 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、次の両方の条件が満たされるまで、インテリジェント アプリケーション バイパス（IAB）およびレート制限を含む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る。
- 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。

アプリケーション コントロール ルールの順位付けに関するガイドラインについては、アプリケーション制御に関する推奨事項を参照してください。

### アプリケーションや他のルールより前に配置される URL ルール

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

### 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、Zoho）

一部のアプリケーションは、複数のプロトコルを使用します。このようなアプリケーションのトラフィックを制御するには、関連するすべてのオプションがアクセス コントロール ポリシーの対象となっていることを確認します。次に例を示します。

- Skype：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制御できるようになります。
- Zoho：Zoho メールを制御するには、[使用可能なアプリケーション（Available Application）] リストから [Zoho] と [Zohoメール（Zoho mail）] の両方を選択します。

### 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。

### 回避的アプリケーション トラフィックの制御

用途別の注意事項と制限事項 （25 ページ）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

アプリケーション検出に関する特別な考慮事項

## 用途別の注意事項と制限事項

- Office 365 管理者用ポータル：

  制限：アクセスポリシーのロギングが最初と最後で有効になっている場合、最初のパケットは Office 365 として検出され、接続の終了は Office 365 管理者用ポータルとして検出されます。これがブロッキングに影響を与えないようにする必要があります。

- Skype:

  アプリケーション制御のガイドラインと制限事項 （22 ページ）を参照してください

- GoToMeeting

  GoToMeeting を完全に検出するには、ルールに次のすべてのアプリケーションが含まれている必要があります。

  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting プラットフォーム
  - LogMeIn
  - STUN

- Zoho:

  アプリケーション制御のガイドラインと制限事項 （22 ページ）を参照してください

- Bittorrent、Tor、Psiphon、および Ultrasurf などの回避的なアプリケーションの場合：

  回避的なアプリケーションの場合、デフォルトでは、信頼性の高いシナリオのみが検出されます。このトラフィックに対するアクション（ブロックや QoS の実装など）を実行する必要がある場合、より効果の高い、さらに積極的な検出の設定が必要なことがあります。これを実行する場合、設定の変更によって誤検出が発生する可能性がありますので、TAC に問い合わせて設定を確認してください。

## アプリケーション制御ルールのトラブルシューティング

アプリケーション コントロール ルールが予想どおりに機能しない場合は、このセクションで説明されているガイドラインを確認してください。

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーションアクセスを許可またはブロックするには、アクセス コントロール ルールで [ポート（Port）]（[選択した宛先ポート（Selected Destination Port）]）条件を使用します。

たとえば、インターネット（安全性が低い）から内部ネットワーク（安全性が高い）への ICMP トラフィックを許可します。

- ユーザ グループによるアプリケーションへのアクセスを許可またはブロックするには、アクセス コントロール ルールで [アプリケーション（Application）] 条件を使用します。

  たとえば、契約業者グループのメンバーによる Facebook へのアクセスをブロックします。

**注意** アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

次の表に、アクセス コントロール ルールを設定する方法の例を示します。

| コントロールの種類 | 操作 | ゾーン、ネットワーク、VLAN タグ | Users | アプリケーション | ポート | URL | SGT/ISE 属性 | インスペクション、ロギング、コメント |
|---|---|---|---|---|---|---|---|---|
| アプリケーションがポート（SSH など）を使用する場合の、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション | お客様の選択（この例では [許可（Allow）]） | 外部インターフェイスを使用する宛先ゾーンまたはネットワーク | 任意（Any） | 設定しない | 使用可能なポート：**SSH**<br>[選択した宛先ポート（Selected Destination Port）] に追加 | 任意（Any） | ISE/ISE-PIC でのみ使用。 | 任意（Any） |

| コントロールの種類 | 操作 | ゾーン、ネットワーク、VLAN タグ | Users | アプリケーション | ポート | URL | SGT/ISE 属性 | インスペクション、ロギング、コメント |
|---|---|---|---|---|---|---|---|---|
| アプリケーションがポートを使用していない場合の（ICMP など）、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション | お客様の選択（この例では [許可（Allow）]） | 外部インターフェイスを使用する宛先ゾーンまたはネットワーク | 任意（Any） | 設定しない | 選択された宛先ポート プロトコル：**ICMP** タイプ：**Any** | 設定しない | ISE/ISE-PIC でのみ使用。 | 任意（Any） |
| ユーザ グループによるアプリケーション アクセス | お客様の選択（この例では [ブロック（Block）]） | お客様の選択 | ユーザグループ（この例では契約業者グループ）を選択。 | アプリケーションの名前（この例では [Facebook]）を選択。 | 設定しない | 設定しない | ISE/ISE-PIC でのみ使用。 | お客様の選択 |

**関連トピック**

ルールの順序指定のガイドライン （41 ページ）

# URL 条件（URL フィルタリング）

URL 条件を使用して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。

詳細については、URL Filteringを参照してください。

# 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。

（注） ISE-PIC アイデンティティ ソースでは、ISE 属性データを提供しません。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられ**なかった** SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とはみなされず、ISE をアイデンティティ ソースとして使用していない場合にのみ機能します。カスタム SGT 条件 （33 ページ）を参照してください。

### 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 | はい | はい |
| SSL | はい | いいえ（No） |

| 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 |
|---|---|---|
| QoS | はい | はい |

**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/ISE-PIC アイデンティティ ソース
ターミナル サービス（TS）エージェントのアイデンティティ 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、TS エージェント、または ISE/ISE-PIC 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/ISE-PIC、ユーザ エージェント、および TS 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。

（注） ISE SGT 属性ルール条件を設定する場合、レルムの設定は任意です。ISE SGT 属性ルール条件は、アイデンティティ ポリシー（レルムの呼び出し元）が関連付けられているかどうかにかかわらず、ポリシー内で設定できます。

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、QoS）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。

QoSルールでユーザ条件を設定する前に、QoSポリシーの対象となるデバイスが、デバイスに適用されたアクセス制御ポリシーで定義されている正しいアイデンティティポリシーを使用していることを確認する**必要があります**。同じデバイスに適用されたQoSポリシーとアクセス制御ポリシーは明示的にリンクされていないため、QoSルールエディタで無効なレルム、ユーザ、およびグループを選択することが可能です。これらの無効な要素は、Firepower Management Centerに存在するが、QoS対象のデバイスには適用されないアイデンティティポリシーから取得された要素です。これらの要素を使用すると、実際に適用されるまで、無効な選択をしたことが判別されません。

## 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| 任意 | Control | いずれか（Any） | いずれか（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。

### 始める前に

- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （28 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。

**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** [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。

### 次のタスク

- 設定変更を展開します。設定変更の展開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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| 任意 | Control | いずれか（Any） | いずれか（Any） | Admin/Access Admin/Network Admin |

### 始める前に

- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （28 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。

**ステップ 1** ルール エディタで、ISE 属性条件のタブをクリックします。

- アクセス コントロール：[SGT/ISE 属性（SGT/ISE Attributes）] タブをクリックします。
- QoS：[ISE 属性（ISE Attributes）] タブをクリックします。

ISE 属性条件を制約するために、ISE 割り当てセキュリティ グループ タグ（SGT）を使用できます。アクセス コントロール ルールでカスタム SGT を使用するには、カスタム SGT 条件 （33 ページ）を参照してください。

**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 ISE メタデータ（AvailableISE Metadata）] [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。

### 次のタスク

- 設定変更を展開します。設定変更の展開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/ISE-PIC アイデンティティ ソースのトラブルシューティング
- TS 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
- 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ト

### 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、TS エージェント、または ISE/ISE-PIC 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、TS エージェント、または ISE/ISE-PIC 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。

### ルールがすべての ISE/ISE-PIC 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/ISE-PIC 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/ISE-PIC ユーザに対するユーザ制御は実行できません。

### ユーザとグループによる大量のメモリの使用

ユーザとグループの処理によって大量のメモリが使用されている場合、**/var/log/messages** に次のようなメッセージが表示されます。

```
UserGroup [WARN] User/Group mem usage is above 80 percent
```

別のメッセージには、ユーザとグループによって使用されているメモリのパーセンテージが表示されます。

こうしたメッセージの表示が続く場合には、次のオプションのいずれかを実行できます。

- アクセス コントロール ポリシーによって処理されるユーザを制限します。
- 管理対象デバイスをメモリが大きなモデルにアップグレードします。

# カスタム SGT 条件

ID ソースとして ISE/ISE-PIC を設定しない場合、ISE によって指定**されていない**セキュリティ グループ タグ（SGT）使用してトラフィックを制御できます。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。

カスタム SGT ルールの条件では、システムが ISE サーバとの接続によって取得した ISE SGT ではなく、手動で作成された SGT オブジェクトを使ってトラフィックをフィルタ処理します。この手動で作成された SGT オブジェクトは、制御するトラフィックの SGT 属性に対応します。カスタム SGT を使用したトラフィック制御は、ユーザ制御とは見なされません。

### カスタム SGT 条件を持つルール

次のルールがカスタム SGT 条件をサポートしています。

- アクセス コントロール
- QoS

## ISE SGT とカスタム SGT ルール条件との比較

ルールの中には、割り当てられた SGT に基づいてトラフィックを制御するために使用できるものがあります。ルールのタイプ、およびアイデンティティ ソースの設定によって、ISE 割り当ての SGT またはカスタム SGT のいずれかを使用して、トラフィックを割り当て済み SGT 属性と照合することができます。

（注） ISE SGT を使用してトラフィックを照合する場合、パケットに SGT 属性が割り当てられていないとしても、パケットの送信元 IP アドレスが ISE 内で既知であれば、そのパケットは ISE SGT ルールと照合されます。

| 条件タイプ | 要件 | ルール エディタにリストされている SGT |
|---|---|---|
| ISE SGT | ISE アイデンティティ ソース | ISE サーバをクエリして取得され、メタデータが自動的に更新される SGT |
| カスタム SGT | ISE/ISE-PIC アイデンティティ ソースなし | ユーザが作成するスタティック SGT オブジェクト |

### 関連トピック

ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （28 ページ）

## カスタムセキュリティグループタグ（SGT）からISEセキュリティグループタグ（SGT）への自動遷移

カスタム SGT に一致するルールを作成し、ISE/ISE-PIC を ID ソースに設定すると、システムは次の動作をします。

- オブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オプションを無効にします。システムは既存の SGT オブジェクトをそのまま保持しますが、それらの変更や、新しいオブジェクトの追加はできません。
- カスタム SGT 条件の既存のルールを保持します。ただし、これらのルールはトラフィックの照合を行いません。また、既存のルールにカスタム SGT 基準を追加することや、カスタム SGT 条件を含む新しいルールを作成することはできません。

ISE を設定する場合は、カスタム SGT 条件を含む既存のルールは削除するか、無効にすることを推奨します。SGT 属性を持つトラフィックを照合するには、代わりに ISE 属性条件を使用します。

### 関連トピック

ユーザ制御用 ISE/ISE-PIC の設定

## カスタム SGT 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| 任意 | Control | いずれか（Any） | いずれか（Any） | Admin/Access Admin/Network Admin |

次の手順では、ISEによって割り当てられて**いない**SGT属性がタグ付けされたトラフィックをフィルタ処理する方法を説明します。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。ISE SGT とカスタム SGT ルール条件との比較 （34 ページ）を参照してください。

### 始める前に

- ISE/ISE-PIC 接続を無効にします。カスタム SGT の照合は、アイデンティティ ソースとして ISE/ISE-PIC を使用する場合、機能しません。
- 一致させる SGT に対応するセキュリティ グループ タグ オブジェクトを設定します。セキュリティ グループ タグ オブジェクトの作成を参照してください。

---

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

**ステップ 2** [Available Attributes] リストから [Security Group Tag] を選択します。

**ステップ 3** [Available Metadata] リストで、カスタム SGT オブジェクトを見つけて選択します。

[すべて（Any）] を選択すると、ルールはSGT属性があるすべてのトラフィックと一致します。たとえば、この値は、TrustSec向けに構成されていないホストからのトラフィックをブロックするアクセス コントロール ルールが必要な場合に選択できます。

**ステップ 4** [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。

---

### 次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

## カスタム SGT 条件のトラブルシューティング

予期しないルールの動作に気付いたら、カスタム SGT オブジェクトの設定を調整することを検討してください。

### 使用不可のセキュリティ グループ タグ オブジェクト

カスタム SGT オブジェクトは、ISE/ISE-PIC をアイデンティティ ソースとして設定していない場合にのみ使用できます。詳細については、「カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移 （34 ページ）」を参照してください。

# 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | いずれか（Any） | いずれか（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。

---

**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。

---

### 次のタスク

- 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数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | 機能に応じて異なる | いずれか（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またはインターフェイスグループの条件）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。

QoS ルールは、常にインターフェイスで制約されます。

**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
プレフィルタリングの設定
QoS ルールの設定
脅威に対する防御のための NAT の設定

# Identify Rules with Issues

展開を防ぐルール（赤色のアイコンでマーく）か、または別のルールがルールの順序で上にあるためにトラフィックが一致することがないルール（黄色のアイコンでマーク）のそれぞれに、システムはフラグを設定します。

**重要** 他のルールに部分的に一致するルールにはフラグが付けられないため、後続の一部のルールが一致しない場合もあります。

**ステップ 1** [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] を選択します。

**ステップ 2** ポリシー名をクリックします。

**ステップ 3** 次のいずれかまたは両方を実行します。

- ウィンドウの上部近くで [警告の表示（Show Warnings）] を探します。

  システムで問題が特定されていない場合、このボタンは表示されません。

  問題がある場合は、このボタンをクリックして問題があるすべてのルールのリストを開きます。

  すべての問題を表示するには、両方のタブ ([ルール エラー（Rule Errors）] と [ルールの警告（Rule Warnings）]) をクリックします。

  下にあるルールのテーブル内からルールを見つけるには、[エラー（Error）] または [警告（Warning）] リストでルール名をクリックします。

- [ルール競合の表示（Show Rule Conflicts）] チェックボックスをオンにします。

  これにより、リスト内で問題があるルールがエラー（赤色）または警告（黄色）のアイコンで示されます。

  必要に応じて、ポリシー内のすべてのルールを確認するまで下にスクロールします。

**ステップ 4** 問題の詳細を表示するには、アイコンの上にポインタを置きます。

**ステップ 5** 部分一致のみであるためフラグが付けられていない重複を検索して対処します。

**ステップ 6** 変更した場合は、[保存（Save）] をクリックするか、または [ルール競合の表示（Show Rule Conflicts）] をいったんオフにしてからもう一度オンにし、変更したルールに競合がないかを評価します。

### 次のタスク

- 問題があるルールを削除または変更し、問題に対処します。
- SSL ポリシーおよび QoS ポリシーで同様のエラーや警告を調べ、問題に対処しあす。

# 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。<br>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。<br>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。 |

| アイコン | 説明 | 例 |
|---|---|---|
| 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伝送します。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、アプリケーションと HTTP 要求が識別されるように接続が確立されます。 |

**関連トピック**

アプリケーション制御のガイドラインと制限事項 （22 ページ）
URL フィルタリングのガイドラインと制限事項

# 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、アプリケーションと HTTP 要求が識別されるように接続が確立されます。

**関連トピック**

アプリケーション制御のガイドラインと制限事項 （22 ページ）
URL フィルタリングのガイドラインと制限事項

# 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。

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。

アプリケーション検出の推奨事項については、アプリケーション制御に関する推奨事項を参照してください。

### 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。

  Certain Firepower Management Center モデルはハードウェアで SSL 暗号化と復号化を実行します。これによりパフォーマンスが大きく向上します。詳細については、TLS 暗号化アクセラレーションを参照してください。

- 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

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。通常、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する必要があります。

例外については、次の項で説明します。

## 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。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 1 URL www.netflix.com をレート制限

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。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 2 URL www.netflix.com をレート制限

### 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（Good CA）が悪意のあるエンティティ（Bad CA）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。

ルールにアプリケーション条件が含まれている場合は、アプリケーション制御に関する推奨事項も参照してください。

### 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。

（注） 特定の管理対象デバイスはハードウェアの TLS/SSL トラフィックの暗号化と復号化をサポートしているため、パフォーマンスが大幅に向上します。詳細については、TLS 暗号化アクセラレーションを参照してください。

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。ただし、重要な例外と注意事項をアクセス コントロール ルールのモニタ アクションで確認してください。
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、およびレート制限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、およびレート制限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 の制限を制御するルールは、セーフサーチ制限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。結果として、YouTube EDU がさらに上位の評価優先順位を持つルールで有効にされていない限り、YouTube トラフィックはセーフサーチ 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。

### 関連トピック

コンテンツ制限について

## アプリケーション ルールの順序

アプリケーション条件を使用するルールは、ルールのリストでより低い順序に移動すると、トラフィックに一致する可能性が高くなります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要がありま

す。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

詳細および例については、アプリケーション制御に関する推奨事項を参照してください。

## SSL ルールの順序

通常、特定の条件（IPアドレスとネットワークなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けします。

### 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

一部のアプリケーションでは、アプリケーション自体に元のサーバ証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで TLS/SSL ルールを設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL ピニングが行われていることを確認するには、Facebook などのモバイル アプリケーションへのログインを試みます。ネットワーク接続エラーが表示された場合は、Web ブラウザを使用してログインします。（たとえば、Facebook のモバイル アプリケーションにログインすることはできませんが、Safari または Chrome を使用して Facebook にログインすることはできます）。Firepower Management Center の接続イベントは、TLS/SSL ピニングのさらなる証明として使用できます

（注） TLS/SSL ピニングはモバイル アプリケーションに限定されません。

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。

### ClientHello の変更の優先順位付け

ClientHello の変更を優先順位付けするには、ServerHello またはサーバ証明書条件に一致するルールの前に、ClientHello メッセージで使用可能な条件に一致するルールを配置します。

管理対象デバイスが SSL ハンドシェイクを処理するときに、ClientHello メッセージを変更して、復号化の可能性を高めることができます。たとえば、FirePOWER システムは圧縮されたセッションを復号化できないので、圧縮メソッドを削除できます。

システムは [復号 - 再署名（Decrypt - Resign）] アクションを含む SSL ルールに最終的に一致させることができる場合、ClientHello メッセージを変更するのみです。システムが新しいサーバへの暗号化セッションを最初に検出したときは、サーバ証明書データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。同じクライアントからの後続の接続で、システムはサーバ証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

ServerHello またはサーバ証明書条件（証明書、識別名、証明書のステータス、暗号スイート、バージョン）と一致するルールを、ClientHello 条件（ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、URL カテゴリ）と一致するルールの前に配置する場合、ClientHello の変更をプリエンプション処理し、復号されないセッションの数を増やすことができます。

#### SSL ポリシーがバイパスされる状況

SSL ポリシーは、[信頼（Trust）]、[ブロック（Block）]、または [リセットしてブロック（Block With Reset）] のアクションを持つアクセス コントロール ルールが次に当てはまる場合、それらのルールに一致する接続に関してバイパスされます。

- セキュリティ ゾーン、ネットワーク、地理位置情報、およびポートだけをトラフィック照合基準として使用する。
- 検査を必要とする他のルール（アプリケーションまたは URL に基づいて接続を照合するルールなど）に先立つか、侵入またはファイル検査を適用するルールを許可する。

## URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

# 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。

# 大規模接続（フロー）のオフロード

データセンターの Firepower 4100/9300 シャーシ で Firepower Threat Defense を展開する場合、ハードウェアにオフロードされるトラフィックの選択を有効にできます。これは、Firepower Threat Defense デバイスのソフトウェアや CPU で処理されないことを意味します。

トラフィックがNIC自体で切り替えられる超高速パスにオフロードされるトラフィックを識別して選択できます。これは、静的フローオフロードと呼ばれます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

- ハイパフォーマンス コンピューティング（HPC）調査サイト。ここでは、Firepower Threat Defense デバイスがストレージと高コンピューティング ステーション間で展開されます。1 つの調査サイトが NFS 経由の FTP ファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータ トラフィックがすべての接続に影響を与えます。NFS を介するFTPファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。
- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、Firepower Threat Defenseデバイスがワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりませんが、遅延は大きな問題です。

フローのオフロードを信頼を含む複数の条件に基づいて Firepower Threat Defense に許可することもできます。これは、動的フロー オフロードと呼ばれます。

Firepower 4100/9300 シャーシでは、以下の基準を満たす接続をオフロードできます。

- （静的フロー オフロードのみ）プレフィルタ ポリシーにより FastPath される。
- （動的フロー オフロードのみ）。インスペクション エンジンが検査の必要がなくなったと判断した検査済みのフロー。これらのフローには次が含まれます。
  - アクセス コントロール ポリシーの [信頼（Trust）] ルール アクションに一致するフロー。
  - インテリジェントアプリケーションバイパス（IAB）ポリシーで、明示的か、またはフロー バイパスのしきい値を超えているために信頼されているフロー。
  - ファイルポリシーまたは信頼ポリシーに一致し、そのフローが信頼できると判断されたフロー。
- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。

（注） PPTP GRE 接続はオフロードされません。

- 標準または 802.1Q タグ付きイーサネット フレームのみ。
- スイッチドまたはルーテッドインターフェイスのみ。パッシブ、インライン、インライン タップ インターフェイスではサポートされません。

さらに、動的フロー オフロードは以下をサポートします。

- FTP データ転送などのセカンダリ接続（可能な限り）。
- 次の IPS プリプロセッサが検査したフロー：
  - SSL、SSH、および SMTP。
  - FTP プリプロセッサのセカンダリ接続。
  - Session Initiation Protocol（SIP）プリプロセッサのセカンダリ接続。
- キーワードを使用する侵入ルール（オプションとも呼ばれる）。
- インテリジェントアプリケーションバイパス（IAB）。特定の条件を満たす場合に、追加検査なしでネットワークの通過を信頼するアプリケーションを特定します。

### 静的フロー オフロードの使い方

オフロードに適格なフローを識別するには、**FastPath** アクションを適用するプレフィルタ ポリシー ルールを作成します。TCP/UDP にはプレフィルタ ルールを使用し、GRE にはトンネル ルールを使用します。ちなみに、セキュリティ ゾーン、送信元と宛先のネットワーク、およびポートのマッチングのみに基づいて [信頼（Trust）] アクションを適用するようにアクセス コントロール ルールを設定し、[セキュリティ インテリジェンス（Security Intelligence）] を無効にする場合、これらのルールをマッチングするフローも、オフロードに適格なフローになります。

接続が確立されると、オフロードに適格な接続であれば、さらなる処理が Firepower Threat Defense ソフトウェアではなく NIC で行われます。 オフロードされたフローは、引き続き制限付きステートフルインスペクション（基本的なTCPフラグおよびオプションのチェックなど）を受信します。システムは必要に応じてさらなる処理のためにファイアウォール システムへのパケットを選択的に増やすことができます。

オフロードされたフローのリバース フローもオフロードされます。

### 動的フロー オフロードの使い方

動的フロー オフロードはデフォルトで有効です。

（注） 動的フローオフロード条件に一致する2つ以上のフローが、同時にオフロードにキューイングされた場合、衝突が発生します。衝突が発生した場合は、最初のフローのみがオフロードします。他のフローは通常どおりに処理されます。**show flow-offload flow** コマンドはコリジョンの統計情報を表示します。

次に、動的オフロードの無効化の例を示します。

```
> configure flow-offload dynamic whitelist disable
```

次に、動的オフロードの有効化の例を示します。

```
> configure flow-offload dynamic whitelist enable
```

## フロー オフロードの制限事項

すべてのフローをオフロードできるわけではありません。オフロードの後でも、フローを特定の条件下でのオフロードから除外することができます。次に、制限事項の一部を示します。

### オフロードできないフロー

次のタイプのフローはオフロードできません。

- IPv6 アドレッシングを使用するフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。

（注） PPTP GRE 接続はオフロードできません。

- パッシブ、インラインまたはインライン タップ モードで設定されたインターフェイス上のフロー。ルーテッド インターフェイスおよびスイッチ インターフェイスがサポートされている唯一のタイプです。
- Snort またはその他のインスペクション エンジンによるインスペクションが必要なフロー。FTP など場合によっては、コントロール チャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- IPsec および VPN 接続。
- 存続可能時間（TTL）値を減少させるフロー。
- 暗号化または復号化を必要とするフロー。
- マルチキャスト フロー。
- TCP インターセプト フロー。
- AAA 関連のフロー。
- Vpath、VXLAN 関連のフロー。

- URL フィルタリング。
- Tracer フロー。
- セキュリティ グループでタグ付けされたフロー。
- クラスタで非対称フローが発生した場合に備えて、別のクラスタ ノードから転送されるリバース フロー。
- クラスタ内の一元化されたフロー（フローのオーナーがマスターでない場合）。

**動的にオフロードできない追加のフロー**

IP オプションを含むフローは動的にオフロードできません。

ダイナミック フローのオフロードによってすべての TCP ノーマライザのチェックが無効になります。

**オフロードを無効にする条件**

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合に Firepower Threat Defense デバイス に返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。
- これらは等コストマルチパス（ECMP）ルーティングの対象であり、入力パケットは 1 つのインターフェイスから別のインターフェイスに移動する。

# ルール管理の履歴：共通の特性

| 機能 | バージョン | 詳細 |
|---|---|---|
| URL の条件に関する情報を新しい「URL フィルタリング」の章に移動 | 6.3 | URL フィルタリングに関する情報を、URL の条件に関する専用トピックを含めてURL Filteringに移動。 |