FirePOWER デバイスのルールの展開について

内容

はじめに

このドキュメントでは、Firepower Management Center(FMC)から展開された場合のセンサーへのアクセスコントロールルール(ACL)の変換について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識
- FMCでのアクセスコントロールポリシーの設定に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Center(FMC)バージョン6.0.0以降
- ソフトウェアバージョン6.0.1以降を実行しているASA Firepower Defenseイメージ(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)
- ソフトウェアバージョン6.0.0以降を実行しているASA Firepower SFRイメージ(ASA 5515-

X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)

- Firepower 7000/8000シリーズセンサーバージョン6.0.0以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

アクセスコントロールルールは、次のパラメータの1つまたは複数の組み合わせを使用して作成されます。

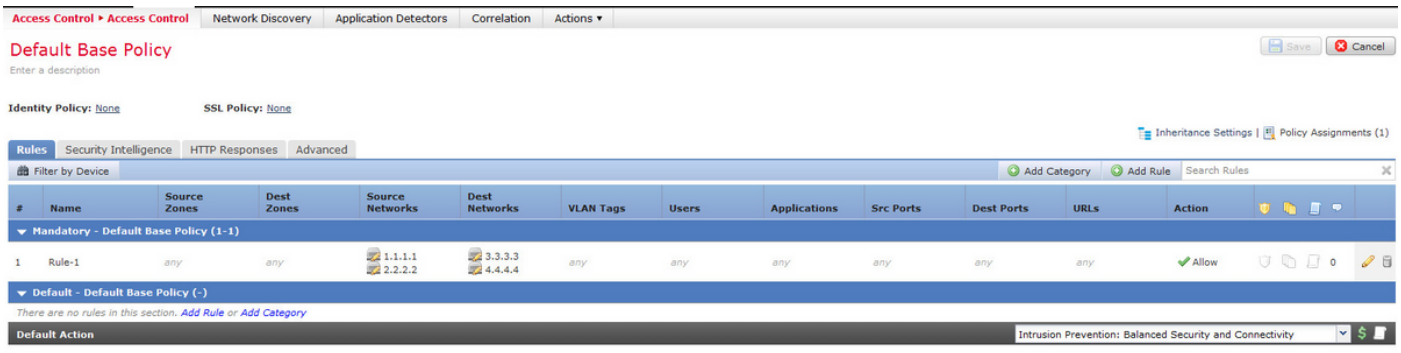
- IPアドレス（送信元および宛先）
- ポート（送信元および宛先）
- URL（システム提供カテゴリおよびカスタムURL）
- アプリケーションディテクタ
- VLAN
- ゾーン

アクセスルールで使用されているパラメータの組み合わせに基づいて、ルールの展開はセンサーで変更されます。このドキュメントでは、FMC上のさまざまなルールの組み合わせと、センサー上のそれぞれの関連する展開について説明します。

ルールの展開について

IPベースのルールの拡張

図に示すように、FMCからのアクセスルールの設定を検討します。



これは、Management Centerの単一のルールです。ただし、センサーに展開すると、図に示すように、4つのルールに展開されます。

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
```

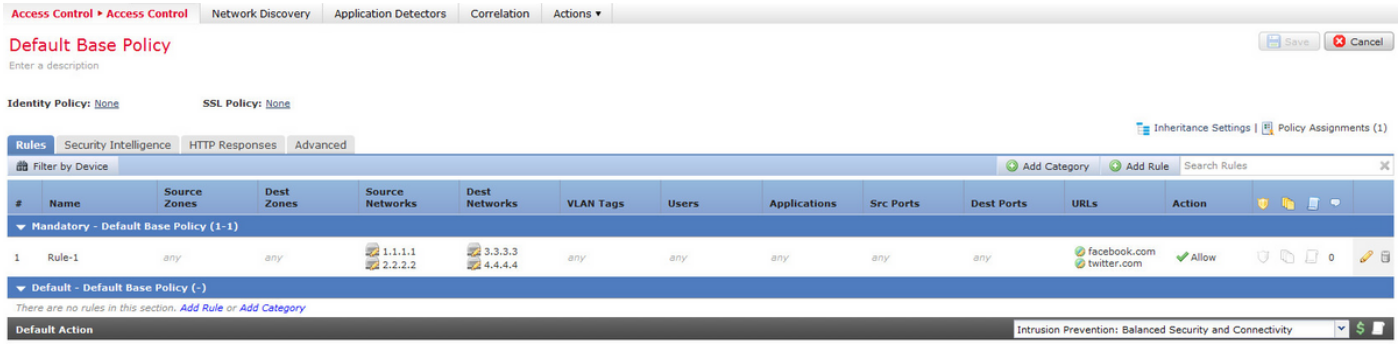
```
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

2つのサブネットが送信元として設定され、2つのホストが宛先アドレスとして設定されたルールを展開すると、このルールはセンサー上で4つのルールに拡張されます。

注：宛先ネットワークに基づいてアクセスをブロックする必要がある場合は、Security Intelligenceのブラックリスト機能を使用するほうが効果的です。

カスタムURLを使用したIPベースルールの拡張

図に示すように、FMCからのアクセスルールの設定を検討します。



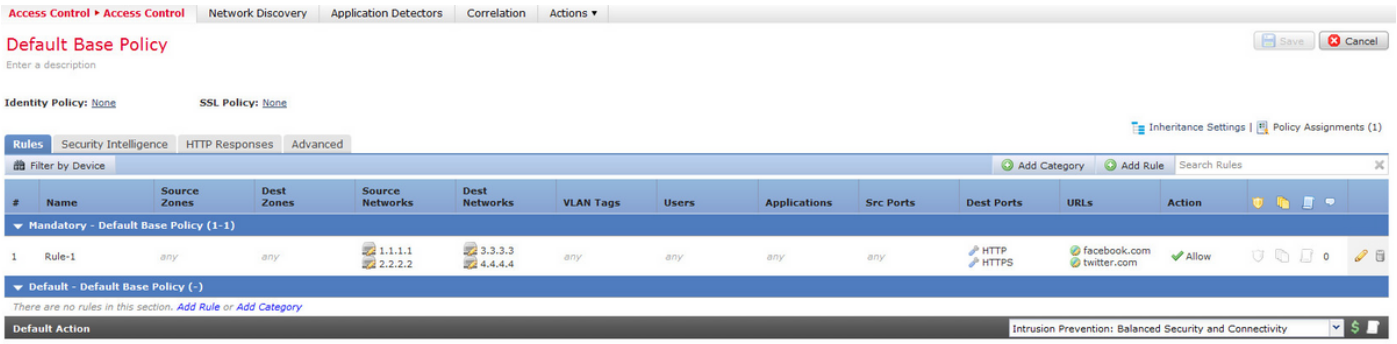
これは、Management Centerの単一のルールです。ただし、センサーに展開した後、図に示すように8つのルールに展開されます。

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "facebook
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "twitter.
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "facebook
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "twitter.
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "facebook
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "twitter.
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "facebook
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "twitter.
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

送信元として設定された2つのサブネット、宛先アドレスとして設定された2つのホスト、およびManagement Center(MC)上の1つのルール内の2つのカスタムURLオブジェクトを含むルールを展開すると、このルールはセンサー上の8つのルールに拡張されます。つまり、カスタムURLカテゴリごとに、送信元と宛先のIP/ポート範囲の組み合わせが設定され、作成されます。

ポートを使用したIPベースルールの拡張

図に示すように、FMCからのアクセスルールの設定を検討します。



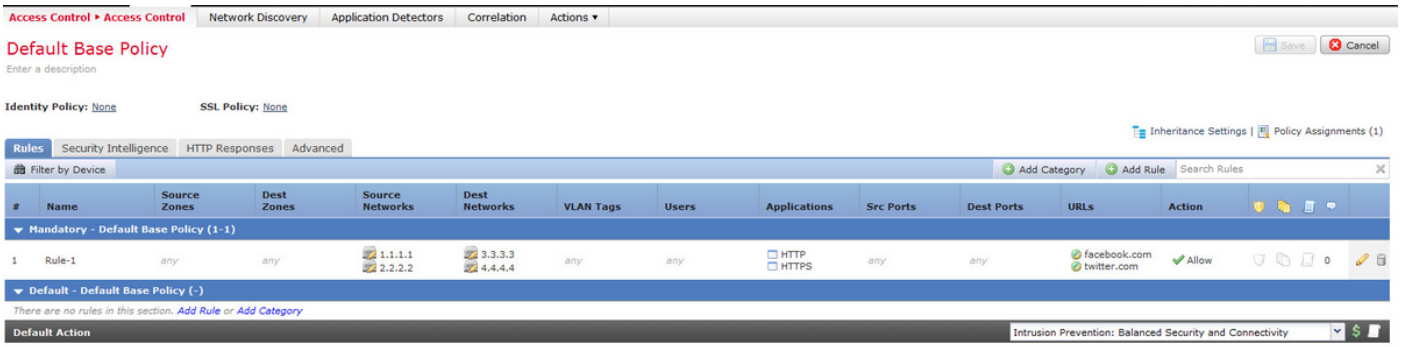
これは、Management Centerの単一のルールです。ただし、センサーに展開した後、図に示すように、16個のルールに展開されます。

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "facebook.com
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "twitter.com"
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "facebook.co
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "twitter.com
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "facebook.com
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "twitter.com"
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "facebook.co
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "twitter.com
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "facebook.com
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "twitter.com"
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "facebook.co
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "twitter.com
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "facebook.com
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "twitter.com"
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "facebook.co
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "twitter.com
268435456 allow any any any any any any any any (ipspolicy 2)
```

送信元として設定された2つのサブネット、宛先アドレスとして設定された2つのホスト、および2つのポートを宛先とする2つのカスタムURLオブジェクトを含むルールを展開すると、このルールはセンサー上で16個のルールに拡張されます。

> 注：アクセスルールのポートを使用する必要がある場合は、標準アプリケーションに存在するアプリケーションディテクタを使用してください。これにより、効率的な方法でルールを拡張できます。

図に示すように、FMCからのアクセスルールの設定を検討します。

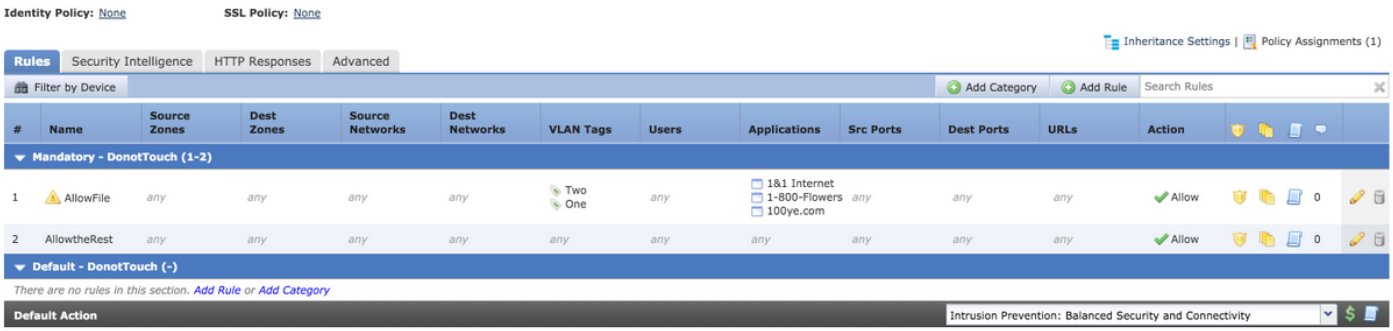


ポートの代わりにアプリケーションディテクタを使用すると、図に示すように、拡張ルールの数は16から8に減少します。

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
```

VLANを使用したIPベースルールの拡張

図に示すように、FMCからのアクセスルールの設定を検討します。



ルールAllowFileには、2つのVLAN IDに一致する1行があり、一部のアプリケーションディテクタ、侵入ポリシー、およびファイルポリシーが含まれています。 ルールAllowFileが2つのルールに展開されます。

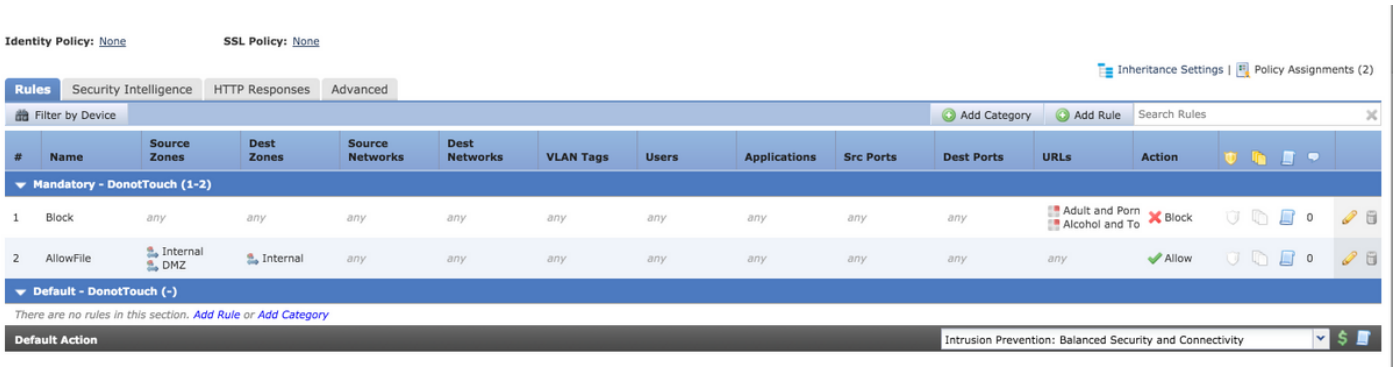
```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena
```

IPSポリシーとファイルポリシーはアクセスコントロールルールごとに固有ですが、複数のアプ

リケーションディテクタが同じルール内で参照されるため、拡張には参加しません。2つのVLAN IDと3つのアプリケーションディテクタを持つルールを検討する場合、各VLANに1つずつ、合計2つのルールしかありません。

URLカテゴリによるIPベースのルールの拡張

図に示すように、FMCからのアクセスルールの設定を検討します。



ブロックルールは、アダルトおよびポルノのすべてのレピュテーションとアルコールおよびタバコのレピュテーション1-3のURLカテゴリをブロックします。これはManagement Center上の単一のルールですが、センサーに展開すると、次に示すように2つのルールに展開されます。

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep le 60)
```

2つのサブネットが送信元として設定され、2つのホストが宛先アドレスとして設定された単一のルールと、2つのURLカテゴリを持つ2つのポートを宛先とする2つのカスタムURLオブジェクトを展開すると、このルールはセンサー上の32のルールに拡張されます。

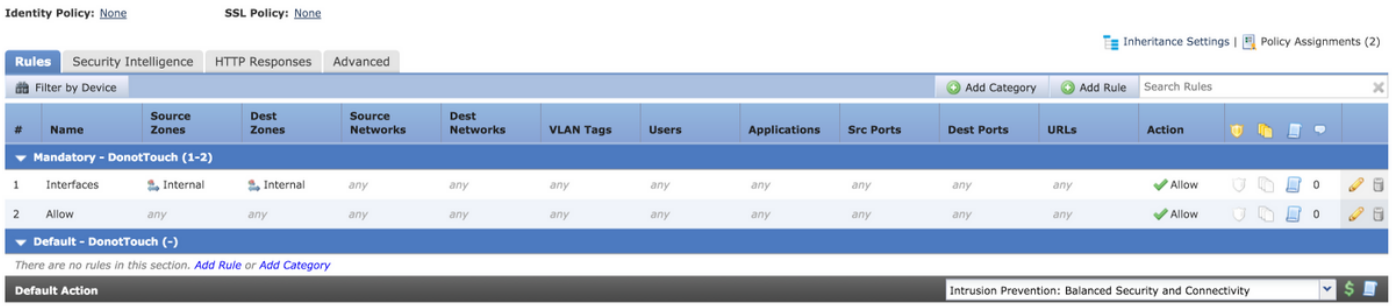
ゾーンを含むIPベースのルールの拡張

ゾーンには、ポリシーで参照される番号が割り当てられます。

ゾーンがポリシーで参照されていても、ポリシーのプッシュ先となるデバイスのインターフェイスにそのゾーンが割り当てられていない場合、そのゾーンはanyと見なされ、anyを指定してもルールは拡張されません。

送信元ゾーンと宛先ゾーンがルール内で同じ場合、ゾーン係数はanyと見なされ、ルールは1つだけ追加されます。これはANYではルールが拡張されないためです。

図に示すように、FMCからのアクセスルールの設定を検討します。



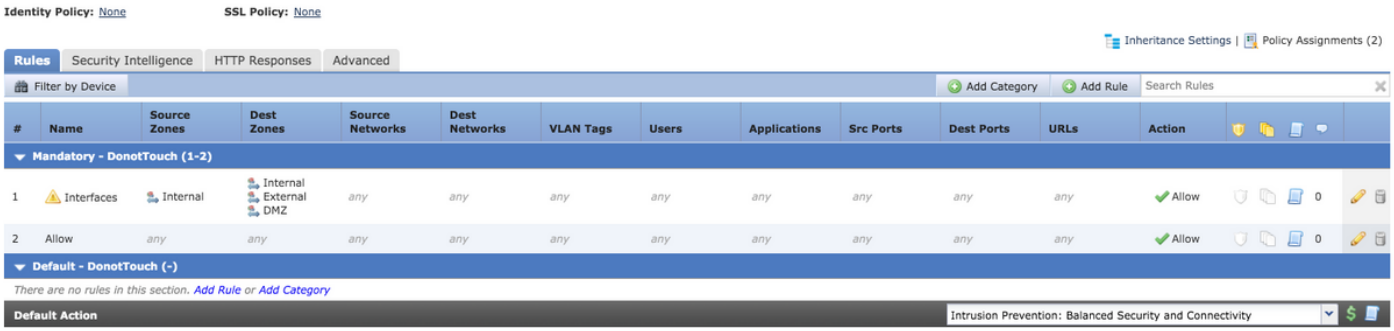
ルールは2つあります。1つのルールにゾーンが設定されているが、送信元ゾーンと宛先ゾーンが同じである。もう一方のルールには、特定の設定はありません。この例では、インターフェイスアクセスルールはルールに変換されません。

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<----------Defa
```

センサーでは、両方のルールが同じように見えます。これは、同じインターフェイスを含むゾーンベースの制御では拡張が行われないためです。

ゾーンベースのアクセス制御規則アクセスの規則の拡張は、規則で参照されているゾーンがデバイス上のインタフェースに割り当てられるときに行われます。

次に示すように、FMCからのアクセスルールの設定を検討します。



ルールInterfacesには、送信元ゾーンを内部、宛先ゾーンを内部、外部、およびDMZとするゾーンベースのルールが含まれます。このルールでは、内部とDMZのインターフェイスゾーンはインターフェイスで設定され、外部はデバイスに存在しません。これは同じことを拡張したものです。

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access rule
268434432 allow any any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<--------Defaul
```

特定のインターフェイスペア(クリアゾーン仕様のInternal > DMZ)に対してルールが作成され、Internal > Internalルールは作成されません。

展開されるルールの数は、有効な関連ゾーン用に作成できるゾーン送信元と宛先のペアの数に比例します。これには、同じ送信元と宛先のゾーンルールが含まれます。

> 注：ポリシーの展開中は、FMCで無効になっているルールは伝搬されず、センサーにも展開されません。

ルール拡張の一般式

センサー上のルール数=（送信元サブネットまたはホストの数）*（宛先Sの数）*（送信元ポートの数）*（宛先ポートの数）*（カスタムURLの数）*（VLANタグの数）*（URLカテゴリの数）*（有効な送信元および宛先ゾーンペアの数）

> 注：計算では、フィールドのany値は1に置き換えられます。ルールの組み合わせの値anyは1と見なされ、ルールは増加も拡張もされません。

ルールの拡張による展開エラーのトラブルシューティング

アクセスルールを追加した後に展開に失敗した場合は、ルールの拡張制限に達している場合は、次の手順に従います

/var/log/action.queue.logで、次のキーワードを含むメッセージを確認します（ログファイル内のエラーはログに記録されません）。

エラー – ルールが多すぎます – ルール28を書き込み、最大ルールは9094です

上記のメッセージは、展開されているルールの数に問題があることを示しています。FMCの設定を確認し、前述のシナリオに基づいてルールを最適化します。

関連情報

- Firepower Management Centerコンフィギュレーションガイド、バージョン6.0
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。