



## ファイアウォールデバイスでのマルチキャストポリシーの設定

マルチキャストのセクションには、セキュリティデバイスに IP マルチキャストルーティングを定義するためのページが含まれています。マルチキャストルーティングは、シングルコンテキストのルーテッドモードでだけサポートされます。

マルチキャストルーティングがイネーブルになれば、デフォルトですべてのインターフェイス上の IGMP と PIM がイネーブルになります。インターネットグループ管理プロトコル (IGMP) は、直接接続されたサブネットにグループのメンバーが存在するかどうかを学習するために使用します。ホストは、IGMP レポートメッセージを送信することにより、マルチキャストグループに参加します。Protocol Independent Multicast (PIM) は、マルチキャストデータグラムの転送テーブルを維持するために使用します。



(注) マルチキャストルーティングでは、UDP トランスポートレイヤだけがサポートされています。

この章は次のトピックで構成されています。

- [PIM および IGMP のイネーブル化 \(1 ページ\)](#)
- [IGMP の設定 \(2 ページ\)](#)
- [マルチキャストルートの設定 \(10 ページ\)](#)
- [マルチキャスト境界フィルタの設定 \(12 ページ\)](#)
- [PIM の設定 \(14 ページ\)](#)

## PIM および IGMP のイネーブル化

[Enable PIM and IGMP] ページを使用すると、セキュリティアプライアンスのすべてのインターフェイスでインターネットグループ管理プロトコル (IGMP) および Protocol Independent Multicast (PIM) をイネーブルまたはディセーブルにできます。IGMP は、直接接続されているサブネット上にグループのメンバーが存在するかどうかを学習するために使用されます。ホストは、IGMP レポートメッセージを送信することにより、マルチキャストグループに参加します。PIM は、マルチキャストデータグラムを転送するための転送テーブルを維持するために使用されます。

このページで [PIMとIGMのイネーブル化 (PEnable PIM and IGMP)] をオンにすると、セキュリティアプライアンスのすべてのインターフェイスで PIM および IGMP がイネーブルになります。このオプションをオフにすると、すべてのインターフェイスで PIM および IGMP がディセーブルになります。



(注) インターフェイスごとに PIM および IGMP をディセーブルにできます。詳細については、[\[IGMP\] ページ - \[Protocol\] タブ \(4 ページ\)](#) および [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#) を参照してください。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクトラから [プラットフォーム (Platform)] > [マルチキャスト (Multicast)] > [PIMとIGMのイネーブル化 (PEnable PIM and IGMP)] を選択します。
- (ポリシービュー) ポリシータイプセレクトラから [PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)] > [マルチキャスト (Multicast)] > [PIMとIGMのイネーブル化 (PEnable PIM and IGMP)] を選択します。共有ポリシー セレクトラから既存のポリシーを選択するか、または新しいポリシーを作成します。

### 関連項目

- [IGMP の設定 \(2 ページ\)](#)
- [マルチキャストルートの設定 \(10 ページ\)](#)
- [マルチキャスト境界フィルタの設定 \(12 ページ\)](#)
- [PIM の設定 \(14 ページ\)](#)

## IGMP の設定

インターネットプロトコルホストは、IGMP を使用して、グループメンバーシップを直接接続されたマルチキャストルータにレポートします。インターネットグループ管理プロトコル (IGMP) は、グループアドレス (クラス D) の IP アドレスを使用します。

ホストグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

[IGMP] ページには、タブ付きのパネルが 4 つあり、Security Manager で IGMP を設定および管理するのに使用できます。

- [\[IGMP\] ページ - \[Protocol\] タブ \(4 ページ\)](#) : このパネルには、インターフェイス固有の IGMP パラメータが表示されます。IGMP をディセーブルにしたり、IGMP パラメータを変更したりできます。
- [\[IGMP\] ページ - \[Access Group\] タブ \(6 ページ\)](#) : インターフェイスで許可されるマルチキャスト送信元を制限するアクセス グループを管理できます。
- [\[IGMP\] ページ - \[Static Group\] タブ \(8 ページ\)](#) : ネットワーク上のホストの中には、IGMP クエリーに応答しないように設定されているものもあります。ただし、その場合でもそのネットワーク セグメントにマルチキャスト トラフィックを転送できます。マルチキャスト トラフィックをネットワーク セグメントにプルする方法が 2 つあります。
  - [\[Join Group\] タブ](#) は、マルチキャスト グループのメンバーとしてインターフェイスを設定するために使用します。この方法では、セキュリティ アプライアンスがマルチキャスト パケットを受け付けて、そのパケットを指定のインターフェイスに転送します。
  - [\[Static Group\] タブ](#) は、スタティックに接続されたグループ メンバーになるようにセキュリティ アプライアンスを設定するために使用します。この方法では、セキュリティ アプライアンスはパケット自体は受け付けず、パケットの転送だけを行います。そのため、スイッチングが高速に実施されます。発信インターフェイスは IGMP キャッシュに表示されますが、インターフェイス自体はマルチキャスト グループのメンバーではありません。

このタブでは、マルチキャストグループをインターフェイスにスタティックに割り当てたり、既存のスタティックなグループ割り当てを変更したりできます。

- [\[IGMP\] ページ - \[Join Group\] タブ \(9 ページ\)](#) : このタブは、セキュリティ アプライアンスが所属するマルチキャストグループを管理するために使用します。



- (注) 単にインターフェイスに特定のグループのマルチキャストパケットを転送するだけで、セキュリティアプライアンスではそのパケットをグループの一部として受け付けないようにする場合は、[\[IGMP\] ページ - \[Static Group\] タブ \(8 ページ\)](#) を参照してください。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセレクトラから [\[プラットフォーム \(Platform\)\]](#) > [\[マルチキャスト \(Multicast\)\]](#) > [\[IGMP\]](#) を選択します。
- (ポリシービュー) ポリシータイプセレクトラから [\[PIX/ASA/FWSMプラットフォーム \(PIX/ASA/FWSM Platform\)\]](#) > [\[IGMP\]](#) を選択します。共有ポリシー セレクトラから既存のポリシーを選択するか、または新しいポリシーを作成します。

## [IGMP] ページ - [Protocol] タブ

[Protocol] タブは、セキュリティ アプライアンス上のインターフェイスに IGMP パラメータを設定するために使用します。

### ナビゲーションパス

[Protocol] タブには、[IGMP] ページからアクセスできます。[IGMP] ページの詳細については、[IGMP の設定 \(2 ページ\)](#) を参照してください。

### 関連項目

- [\[Configure IGMP Parameters\] ダイアログボックス \(5 ページ\)](#)
- [PIM および IGMP のイネーブル化 \(1 ページ\)](#)
- [PIM の設定 \(14 ページ\)](#)
- [マルチキャスト ルートの設定 \(10 ページ\)](#)

### フィールド リファレンス

表 1: [Protocol] タブ

| 要素                          | 説明   |
|-----------------------------|--|
| [Protocol] テーブル             |  |
| インターフェイス                    | IGMP 設定を適用するインターフェイスの名前。   |
| [有効 (Enabled) ]             | インターフェイスで IGMP がイネーブルになっているかどうかを示します。  |
| バージョン                       | インターフェイスでイネーブルになっている IGMP のバージョン。  |
| Query Interval              | 指定ルータが IGMP ホストクエリーメッセージを送信する間隔 (秒数)。有効な値の範囲は 1 ~ 3600 秒です。デフォルト値は 125 秒です。  |
| クエリー タイムアウト (Query Timeout) | 前のセキュリティ アプライアンスがインターフェイスに対するクエリーを停止してから、セキュリティ アプライアンスがその処理を引き継ぐまでの時間 (秒数)。有効な値の範囲は 60 ~ 300 秒です。デフォルト値は 255 秒です。 |

| 要素                       | 説明  |
|--------------------------|---|
| 応答時間 (Response Time)     | IGMP クエリーでアドバタイズされる最大応答時間 (秒数)。セキュリティ アプライアンスが指定された応答時間内にホスト レポートを受信しない場合、IGMP グループは排除されます。この値を小さくすると、セキュリティ アプライアンスによるグループの排除が早くなります。有効な値の範囲は 1 ～ 12 秒です。デフォルト値は 10 秒です。この値の変更は、IGMP Version 2 の場合にだけ有効です。 |
| Group Limit              | インターフェイス上で参加できるホストの最大数。有効な値の範囲は 1 ～ 500 です。デフォルト値は 500 です。  |
| Maximum Groups (PIX 6.3) | マルチキャストがイネーブルになっているグループの最大数。有効な値の範囲は 0 ～ 2000 です。   |
| Forward Interface        | IGMP 転送がイネーブルになっている場合に、選択したインターフェイスが IGMP ホスト レポートを転送するインターフェイスの名前。   |

## [Configure IGMP Parameters] ダイアログボックス

[Configure IGMP Parameters] ダイアログボックスは、セキュリティ アプライアンス上のインターフェイスに IGMP パラメータを設定するために使用します。

### ナビゲーションパス

[Configure IGMP Parameters] ダイアログボックスには、[IGMP] ページ - [Protocol] タブからアクセスできます。詳細については、[\[IGMP\] ページ - \[Protocol\] タブ \(4 ページ\)](#) を参照してください。

### 関連項目

- [\[IGMP\] ページ - \[Protocol\] タブ \(4 ページ\)](#)
- [IGMP の設定 \(2 ページ\)](#)

### フィールドリファレンス

表 2: [Configure IGMP Parameters] ダイアログボックス

| 要素                   | 説明   |
|----------------------|--|
| インターフェイス (Interface) | IGMP 設定を適用するインターフェイスの名前。                               |
| Forward Interface    | IGMP 転送がイネーブルになっている場合に、IGMP ホスト レポートが転送されるインターフェイスの名前。 |

| 要素                         | 説明  |
|----------------------------|---|
| バージョン                      | インターフェイスでイネーブルになっている IGMP のバージョン。IGMP バージョン 1 をイネーブルにするには 1 を選択し、IGMP バージョン 2 をイネーブルにするには 2 を選択します。機能によっては、IGMP バージョン 2 にする必要があります。デフォルトでは、セキュリティ アプライアンスは IGMP バージョン 2 を使用します。                           |
| Query Interval             | 指定ルータが IGMP ホストクエリーメッセージを送信する間隔（秒数）。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。  |
| 応答時間（Response Time）        | IGMP クエリーでアドバタイズされる最大応答時間（秒数）。セキュリティ アプライアンスが指定された応答時間内にホストレポートを受信しない場合、IGMP グループは排除されます。この値を小さくすると、セキュリティ アプライアンスによるグループの排除が早くなります。有効な値の範囲は 1 ～ 12 秒です。デフォルト値は 10 秒です。この値の変更は、IGMP Version 2 の場合にだけ有効です。 |
| Maximum Groups (PIX 6.3)   | マルチキャストがイネーブルになっているグループの最大数。有効な値の範囲は 0 ～ 2000 です。   |
| PIX 7.x、ASA だけ             |   |
| Enable IGMP                | このチェックボックスをオンにすると、指定したインターフェイスで IGMP がイネーブルになります。   |
| Group Limit                | インターフェイス上で参加できるホストの最大数。有効な値の範囲は 1 ～ 500 です。デフォルト値は 500 です。  |
| クエリー タイムアウト（Query Timeout） | 前のセキュリティ アプライアンスがインターフェイスに対するクエリーを停止してから、セキュリティ アプライアンスがその処理を引き継ぐまでの時間（秒数）。有効な値の範囲は 60 ～ 300 秒です。デフォルト値は 255 秒です。   |

## [IGMP] ページ - [Access Group] タブ

[Access Group] タブは、インターフェイスで許可されるマルチキャスト グループを制御するために使用します。

このページのテーブルには、現在定義されているすべてのマルチキャスト アクセス グループがリストされ、グループごとに、グループが定義されているインターフェイスまたはインターフェイス ロールの名前、グループ ネットワーク、およびグループが許可されるか拒否されるかが表示されます。これらのフィールドの詳細については、[\[Configure IGMP Access Group Parameters\] ダイアログボックス（7 ページ）](#) を参照してください。

- マルチキャスト アクセス グループをテーブルに追加するには、[Add Row] ボタンをクリックします。

- グループの設定を編集するには、そのグループを選択して [Edit Row] ボタンをクリックします。
- グループを削除するには、そのグループを選択して [Delete Row] ボタンをクリックします。

#### ナビゲーションパス

[Access Group] タブには、[IGMP の設定 \(2 ページ\)](#) からアクセスできます。

#### 関連項目

- [PIM および IGMP のイネーブル化 \(1 ページ\)](#)
- [マルチキャスト ルートの設定 \(10 ページ\)](#)

## [Configure IGMP Access Group Parameters] ダイアログボックス

[Configure IGMP Access Group Parameters] ダイアログボックスは、アクセス グループ エントリを追加または変更するために使用します。

#### ナビゲーションパス

[Configure IGMP Access Group Parameters] ダイアログボックスには、[\[IGMP\] ページ - \[Protocol\] タブ \(4 ページ\)](#) からアクセスできます。

#### 関連項目

- [\[IGMP\] ページ - \[Protocol\] タブ \(4 ページ\)](#)
- [IGMP の設定 \(2 ページ\)](#)

#### フィールドリファレンス

表 3: [Configure IGMP Access Group Parameters] ダイアログボックス

| 要素                      | 説明   |
|-------------------------|--|
| インターフェイス (Interface)    | アクセス グループを割り当てるインターフェイスの名前を入力するか、または選択します。   |
| Multicast Group Network | 指定したインターフェイスに割り当てるマルチキャストグループアドレスを入力するか、または選択します。1つ以上のIPアドレス/ネットワークマスク エントリ、1つ以上のネットワーク/ホストオブジェクト、または両方の組み合わせを指定できます。エントリはカンマで区切ります。<br><br>グループ ネットワーク アドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。 |

| 要素 | 説明   |
|----|--|
| 操作 | インターフェイスでマルチキャストグループを許可する場合は、[許可 (permit)] を選択します。マルチキャストグループを許可しない場合は、[拒否 (deny)] を選択します。 |

## [IGMP] ページ - [Static Group] タブ

[Static Group] タブは、マルチキャストグループをインターフェイスにスタティックに割り当てるために使用します。

### ナビゲーションパス

[Static Group] タブには、[IGMP] ページからアクセスできます。[IGMP] ページの詳細については、[IGMP の設定 \(2 ページ\)](#) を参照してください。

### 関連項目

- [PIM および IGMP のイネーブル化 \(1 ページ\)](#)
- [マルチキャストルートの設定 \(10 ページ\)](#)
- [PIM の設定 \(14 ページ\)](#)

### フィールドリファレンス

表 4: [Static Group] タブ

| 要素  | 説明                           |
|---|------------------------------|
| インターフェイス (Interface)                        | スタティックグループを関連付けるインターフェイスの名前。 |
| [マルチキャストグループアドレス (Multicast Group Address)] | このルールを適用するマルチキャストグループアドレス。   |

## [Configure IGMP Static Group Parameters] ダイアログボックス

[Configure IGMP Static Group Parameters] ダイアログボックスは、マルチキャストグループをインターフェイスにスタティックに割り当てるため、または既存のスタティックなグループ割り当てを変更するために使用します。

### ナビゲーションパス

[Configure IGMP Static Group Parameters] ダイアログボックスには、[IGMP] ページ - [Static Group] タブからアクセスできます。詳細については、[\[IGMP\] ページ - \[Static Group\] タブ \(8 ページ\)](#) を参照してください。



関連項目

- [\[IGMP\] ページ - \[Static Group\] タブ \(8 ページ\)](#)
- [IGMP の設定 \(2 ページ\)](#)

フィールドリファレンス

表 5: [Configure IGMP Static Group Parameters] ダイアログボックス

| 要素                   | 説明  |
|----------------------|---|
| インターフェイス (Interface) | スタティックグループを関連付けるインターフェイスの名前。  |
| マルチキャストグループ          | このルールを適用するマルチキャストグループアドレス。グループアドレスは、224.0.0.0 ~ 239.255.255.255 の値である必要があります。 |

## [IGMP] ページ - [Join Group] タブ

[Join Group] タブは、マルチキャストグループのメンバーになるようにインターフェイスを設定するために使用します。

ナビゲーションパス

[Join Group] タブには、[IGMP] ページからアクセスできます。[IGMP] ページの詳細については、[IGMP の設定 \(2 ページ\)](#) を参照してください。

関連項目

- [PIM および IGMP のイネーブル化 \(1 ページ\)](#)
- [PIM の設定 \(14 ページ\)](#)
- [マルチキャストルートの設定 \(10 ページ\)](#)

フィールドリファレンス

表 6: [Join Group] タブ

| 要素   | 説明                                  |
|--|-------------------------------------|
| インターフェイス (Interface)                         | マルチキャストグループメンバーシップを設定するインターフェイスの名前。 |
| [マルチキャストグループアドレス (Multicast Group Address) ] | このルールを適用するマルチキャストグループアドレス。          |

## [Configure IGMP Join Group Parameters] ダイアログボックス

[Configure IGMP Join Group Parameters] ダイアログボックスは、マルチキャスト グループのメンバーになるようにインターフェイスを設定するため、または既存のメンバーシップ情報を変更するために使用します。

### ナビゲーションパス

[Configure IGMP Join Group Parameters] ダイアログボックスには、[IGMP] ページ - [Join Group] タブからアクセスできます。詳細については、[\[IGMP\] ページ - \[Join Group\] タブ \(9 ページ\)](#) を参照してください。

### 関連項目

- [\[IGMP\] ページ - \[Join Group\] タブ \(9 ページ\)](#)
- [IGMP の設定 \(2 ページ\)](#)

### フィールドリファレンス

表 7: [Configure IGMP Join Group Parameters] ダイアログボックス

| 要素                   | 説明   |
|----------------------|--|
| インターフェイス (Interface) | マルチキャスト グループ メンバーシップを設定するインターフェイスの名前。  |
| Join Group           | このルールを適用するマルチキャスト グループ アドレス。グループ アドレスは、224.0.0.0 ~ 239.255.255.255 の値である必要があります。 |

## マルチキャスト ルートの設定

スタティックなマルチキャスト ルートを使用すると、マルチキャスト トラフィックとユニキャスト トラフィックとを区別できます。たとえば、送信元と宛先間のパスでマルチキャスト ルーティングがサポートされていない場合、このことを解決するには、マルチキャスト デバイスを 2 つ用意して両者間に GRE トンネルを設定し、そのトンネルでマルチキャスト パケットを送信します。

スタティックなマルチキャスト ルートは、セキュリティ アプライアンスにローカルであり、アドバタイズも再配布もされません。

[Multicast Routes] ページは、スタティックなマルチキャスト ルートを管理するために使用します。現時点で定義されているルートが表示され、スタティックなマルチキャスト ルートを追加、編集、および削除できます。

このページのこのテーブルに表示されているフィールドの詳細については、[\[Add MRoute Configuration\]/\[Edit MRoute Configuration\] ダイアログボックス \(11 ページ\)](#) を参照してください。

#### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから、**[プラットフォーム (Platform)]** > **[マルチキャスト (Multicast)]** > **[マルチキャストルート (Multicast Routes)]** を選択します。
- (ポリシービュー) ポリシータイプセクタから、**[PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)]** > **[マルチキャスト (Multicast)]** > **[マルチキャストルート (Multicast Routes)]** を選択します。共有ポリシーセクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

#### 関連項目

- [PIM および IGMP のイネーブル化 \(1 ページ\)](#)
- [IGMP の設定 \(2 ページ\)](#)
- [PIM の設定 \(14 ページ\)](#)

## [Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックス

[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックスは、スタティックなマルチキャストルートをセキュリティアプライアンスに追加するため、または既存のルートを変更するために使用します。

#### ナビゲーションパス

[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックスには、[\[Multicast Routing\]](#) ページからアクセスできます。詳細については、[マルチキャストルートの設定 \(10 ページ\)](#) を参照してください。

#### フィールドリファレンス

表 8: [Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックス

| 要素                             | 説明  |
|--------------------------------|---|
| 送信元インターフェイス (Source Interface) | マルチキャストルートの着信インターフェイスを入力するか、または選択します。                       |
| 送信元ネットワーク                      | マルチキャスト送信元の IP アドレスおよびマスクを入力するか、またはネットワーク/ホスト オブジェクトを選択します。 |

| 要素                          | 説明   |
|-----------------------------|--|
| Output Interface/Dense      | (任意) マルチキャストルートの発信インターフェイスを入力するか、または選択します。宛先インターフェイスを指定した場合、ルートは選択したインターフェイス経由で転送されます。宛先インターフェイスを指定しない場合、RPF を使用してルートが転送されます。インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。 |
| マルチキャストネットワーク (PIX 6.3)     | マルチキャストパケットを受信するグループを入力するか、または選択します。これは、範囲が 224.0.1.0 ~ 239.255.255.255 のマルチキャスト IP アドレスである必要があります。  |
| Distance (PIX 7.x、ASA、FWSM) | スタティックなマルチキャストルートのアドミニストレーティブディスタンスを入力します。スタティックなマルチキャストルートにユニキャストルートと同じアドミニストレーティブディスタンスがある場合は、スタティックなマルチキャストルートが優先されます。  |

## マルチキャスト境界フィルタの設定

バージョン 7.2(1) 以降が稼働する ASA では、[Multicast Boundary Filter] ページを使用して、マルチキャスト ドメイン間の境界として機能するようにアプライアンスを設定できます。ASA は、マルチキャストグループアドレスをアクセスリストと比較して、リストで特に許可したものを除いてすべてのマルチキャストトラフィックをブロックします。

[Multicast Boundary Filter] ページには、現在定義されているインターフェイス境界フィルタがすべて表示されます。このページから、フィルタリストを追加、編集、および削除できます。

このページのフィールドの詳細については、[\[Add MBoundary Configuration\]/\[Edit MBoundary Configuration\] ダイアログボックス \(13 ページ\)](#) を参照してください。

### ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから、[プラットフォーム (Platform)] > [マルチキャスト (Multicast)] > [マルチキャストバウンダリフィルタ (Multicast Boundary Filter)] を選択します。
- (ポリシービュー) ポリシータイプセクタから、[PIX/ASA/FWSMプラットフォーム (PIX/ASA/FWSM Platform)] > [マルチキャスト (Multicast)] > [マルチキャストバウンダリフィルタ (Multicast Routes)] を選択します。Multicast Boundary Filter 共有ポリシーセクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

### 関連項目

- [\[Add MBoundary Interface Configuration\]/\[Edit MBoundary Interface Configuration\] ダイアログボックス \(13 ページ\)](#)

## [Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックス

[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックスは、個々のインターフェイスのマルチキャスト境界フィルタリストを追加、編集、および削除するために使用します。

### ナビゲーションパス

[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックスには、[マルチキャスト境界フィルタの設定 \(12 ページ\)](#) からアクセスできます。

### 関連項目

- [\[Add MBoundary Interface Configuration\]/\[Edit MBoundary Interface Configuration\] ダイアログボックス \(13 ページ\)](#)
- [マルチキャスト境界フィルタの設定 \(12 ページ\)](#)

### フィールドリファレンス

表 9: [Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックス

| 要素  | 説明  |
|---|---|
| インターフェイス (Interface)  | このマルチキャスト境界のインターフェイスを入力するか、または選択します。  |
| すべてのAuto_RPグループ範囲のアナウンスメントの削除 (any Auto_RP group range announcements) | このボックスをオンにすると、このインターフェイスの境界アクセスコントロールリストによって拒否された Auto-RP メッセージがドロップされます。これは、自動フィルタリングと呼ばれます。   |
| Multicast boundary filter configuration list                          | 指定したインターフェイス用に特に許可または拒否されたマルチキャストグループアドレスを表示します。このリストは、 <a href="#">[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス (13 ページ)</a> ([Add Row or Edit Row] をクリックします) で管理されます。 |

## [Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス

このダイアログボックスは、[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックスのリストに対する許可または拒否を示すマルチキャストグループ エントリを定義するために使用します。

## ナビゲーションパス

[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックスには、[\[Add MBoundary Interface Configuration\]/\[Edit MBoundary Interface Configuration\] ダイアログボックス \(13 ページ\)](#) からアクセスできます。

## 関連項目

- [マルチキャスト境界フィルタの設定 \(12 ページ\)](#)

## フィールド リファレンス

表 10: [Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス

| 要素          | 説明   |
|-------------|--|
| 操作          | [許可 (permit) ] または [拒否 (deny) ] を選択して、このマルチキャストグループに対して実行するアクションを指定します。  |
| マルチキャストグループ | このアクションが適用される単一のマルチキャストアドレス、またはマルチキャストグループアドレスを入力します。アドレスは、0.0.0.0 であるか、または 224.0.0.0 ~ 239.255.255.255 である必要があります。グループアドレス範囲は、標準サブネットマスク (239.0.0.0 255.0.0.0 など) または CIDR プレフィックス表記法 (239.0.0.0/8 など) を使用して入力できます。<br><br>また、指定済みのネットワーク/ホストオブジェクトも選択できます。 |

# PIM の設定

IGMP を使用してマルチキャスト送信を受信するように登録された各ホストに特定のマルチキャスト送信を配布する場合、Protocol Independent Multicast (PIM) を使用すると、ネットワークの最良パスを柔軟に決定できます。ルータおよびセキュリティデバイスは、PIM を使用して、マルチキャスト データグラムを転送するためのテーブルを維持します。

Cisco ルータのデフォルトである PIM Sparse Mode (PIM SM; PIM スパース モード) では、マルチキャスト送信の送信元がブロードキャストを開始すると、登録されたすべてのホストにパケットが到達するまで、トラフィックがマルチキャストルータ間を転送されます。トラフィック送信元により直接的に到達できるパスが存在する場合は、ラストホップルータが Join メッセージを送信元に送信します。これにより、より適切なパスを経由して、トラフィックが再ルーティングされます。



(注) PIM は PAT ではサポートされていません。これは、PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルでだけ機能するためです。

セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、デフォルトではすべてのインターフェイスで PIM および IGMP がイネーブルになります。インターフェイスごとに PIM をディセーブルにできます。

[PIM] ページには、最大 6 個のタブ付きパネルが表示されます。

- [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#) : インターフェイス固有の PIM プロパティを管理できます。
- [\[PIM\] ページ - \[Neighbor Filter\] タブ \(17 ページ\)](#) : 個々のインターフェイスのネイバーフィルタを管理できます。ただし、ASA 7.2(1)+ のデバイスでだけ使用できます。
- [\[PIM\] ページ - \[Bidirectional Neighbor Filter\] タブ \(18 ページ\)](#) : 個々のインターフェイスの双方向ネイバーフィルタを管理できます。ただし、ASA 7.2(1)+ のデバイスでだけ使用できます。
- [\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#) : PIM を設定するときは、ランデブーポイント (RP) として動作するデバイスを 1 つ以上選択する必要があります。RP は、共用配布ツリーの単一の共通ルートであり、デバイスごとにスタティックに設定されます。第 1 ホップ ルータは、RP を使用して、送信元のマルチキャスト ホストに代わって登録パケットを送信します。
- [\[PIM\] ページ - \[Route Tree\] タブ \(23 ページ\)](#) : デフォルトでは、新規送信元から最初のパケットが届くと、PIM リーフ ルータはただちに最短パス ツリーに参加します。これにより、遅延が短縮されます。ただし、共有ツリーよりも多くのメモリが必要になります。セキュリティ アプライアンスが最短パス ツリーに参加するか、または共有ツリーを使用するかについて、すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスだけを対象に設定できます。
- [\[PIM\] ページ - \[Request Filter\] タブ \(24 ページ\)](#) : セキュリティ アプライアンスが RP として機能する場合は、登録できるマルチキャスト送信元を制限できます。これにより、未認可の送信元が RP に登録されることを回避できます。[Request Filter] パネルでは、セキュリティ アプライアンスが PIM 登録メッセージを受け付けるマルチキャスト送信元を定義できます。

## [PIM] ページ - [Protocol] タブ

[Protocol] タブは、セキュリティ アプライアンスでインターフェイスの PIM プロパティを設定するために使用します (ただし、PIX 6.3 デバイスにはありません)。現在設定されているすべてのインターフェイスが表示されます。このパネルでは、エントリを追加、編集、および削除できます。

このパネルのフィールドの詳細については、[\[Add PIM Protocol\]/\[Edit PIM Protocol\] ダイアログボックス \(16 ページ\)](#) を参照してください。

### ナビゲーションパス

[PIM] ページから [Protocol] タブにアクセスします。詳細については、[PIM の設定 \(14 ページ\)](#) を参照してください。

## 関連項目

- [PIM] ページ - [Rendezvous Points] タブ (20 ページ)
- [PIM] ページ - [Route Tree] タブ (23 ページ)
- [PIM] ページ - [Request Filter] タブ (24 ページ)

## [Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックス

[Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックスは、PIX 7.x 以降が稼働するセキュリティ アプライアンスでインターフェイスの PIM プロパティを設定するために使用します。

## 指定ルータについて

代表ルータは、PIM Register、Join、Prune の各メッセージをランデブーポイント (RP) に送信します。ネットワーク セグメントに複数のマルチキャストルーティング デバイスがあるときは、DR プライオリティに基づいて指定ルータを選択する選択プロセスがあります。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。デフォルトでは、セキュリティ アプライアンスの DR プライオリティは 1 です。

## ナビゲーションパス

[Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックスには、[PIM] ページ - [Protocol] タブ (15 ページ) からアクセスできます。

## フィールド リファレンス

表 11 : [Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックス

| 要素   | 説明  |
|--|---|
| インターフェイス (Interface)                         | PIM を設定するインターフェイスを入力するか、または選択します。   |
| Protocol-Independent Multicast (PIM) のイネーブル化 | このチェックボックスをオンにすると、選択したインターフェイスで PIM がイネーブルになります。このチェックボックスをオフにすると、テーブルからこの PIM プロトコル エントリを削除せずに、インターフェイスで PIM をディセーブルにできます。   |
| DR Priority                                  | このインターフェイスの Designated Router (DR; 指定ルータ) プライオリティ。サブネットで DR プライオリティが最も高いルータが指定ルータになります。有効な値の範囲は 0 ~ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値をゼロに設定すると、セキュリティ アプライアンス インターフェイスは、デフォルトルータになる資格がなくなります。 |
| Hello Interval (seconds)                     | インターフェイスが PIM hello メッセージを送信する頻度 (秒)。有効な値の範囲は 1 ~ 3600 秒で、デフォルト値は 30 秒です。   |



| 要素                            | 説明   |
|-------------------------------|--|
| Join-Prune Interval (seconds) | インターフェイスが PIM Join および Prune アドバタイズメントを送信する頻度 (秒)。有効な値の範囲は 10 ~ 600 秒で、デフォルト値は 60 秒です。 |

## [PIM] ページ - [Neighbor Filter] タブ

PIM ネイバー フィルタは、PIM に参加できるネイバー デバイスを定義するアクセス コントロール リスト (ACL) です。インターフェイスのネイバー フィルタが設定されていない場合、制限はありません。PIM ネイバー フィルタが設定されている場合は、フィルタ リストで許可されるネイバーだけが、セキュリティ アプライアンスとともに、PIM に参加できます。

バージョン 7.2(1) 以降が稼働する ASA では、[Neighbor Filter] タブを使用して、PIM ネイバーになることができるデバイスを制御できます。このパネルは、インターフェイスごとのネイバー フィルタ リストを定義および管理するために使用します。このパネルのフィールドの詳細については、[\[Add PIM Neighbor Filter\]/\[Edit PIM Neighbor Filter\] ダイアログボックス \(17 ページ\)](#) を参照してください。

### ナビゲーションパス

[PIM] ページから [Protocol] タブにアクセスします。詳細については、[PIM の設定 \(14 ページ\)](#) を参照してください。

### 関連項目

- [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#)
- [\[PIM\] ページ - \[Bidirectional Neighbor Filter\] タブ \(18 ページ\)](#)
- [\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#)
- [\[PIM\] ページ - \[Route Tree\] タブ \(23 ページ\)](#)
- [\[PIM\] ページ - \[Request Filter\] タブ \(24 ページ\)](#)

## [Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックス

[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックスは、[PIM] ページの [Neighbor Filter] パネルに表示される PIM ネイバー フィルタ ACL でエントリーを追加および編集するために使用します。

### ナビゲーションパス

[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックスには、[\[PIM\] ページ - \[Neighbor Filter\] タブ \(17 ページ\)](#) からアクセスできます。

## フィールド リファレンス

表 12: [Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックス

| 要素                      | 説明  |
|-------------------------|---|
| インターフェイス<br>(Interface) | この PIM ネイバー フィルタ エントリが適用されるインターフェイスを入力するか、または選択します。   |
| Neighbor Filter Group   | 選択したアクションが適用される単一のマルチキャストアドレス、またはマルチキャスト グループ アドレスを入力します。グループ アドレス範囲は、標準サブネットマスク (239.0.0.0 255.0.0.0 など) または CIDR プレフィックス表記法 (239.0.0.0/8 など) を使用して入力できます。<br><br>また、指定済みのネットワーク/ホストオブジェクトも選択できます。 |
| 操作                      | 指定したネイバーを PIM に参加させるには [許可 (permit) ] を選択し、指定したネイバーを PIM に参加させないためには [拒否 (deny) ] を選択します。   |

## [PIM] ページ - [Bidirectional Neighbor Filter] タブ

PIM 双方向ネイバーフィルタは、双方向ツリーおよび Designated Forwarder (DF; 代表フォワーダ) 選択に参加できるネイバーデバイスを定義するアクセス制御リスト (ACL) です。PIM 双方向ネイバーフィルタがインターフェイスに設定されていない場合は、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバーフィルタを使用すると、DF 選択に参加するデバイスを指定し、その一方で、引き続きすべてのデバイスがスパースモードのドメインに参加できるようにして、スパースモード専用ネットワークから「双方向」ネットワークに移行できます。双方向対応デバイスは、セグメントに双方向でないデバイスがあっても、数ある双方向対応デバイスの中から DF を選択できます。双方向でないデバイス上にマルチキャスト境界があるため、双方向グループからの PIM メッセージおよびデータが双方向サブセットクラウドの内外に漏れることを回避できます。

双方向 PIM を使用すると、マルチキャスト デバイスが保持する状態情報を削減できます。セグメント内のすべてのマルチキャスト デバイスが、DF を選択できるように双方向対応である必要があります。

PIM 双方向ネイバー フィルタがイネーブルになっていると、ACL で許可されるルータおよび他のデバイスは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。

- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

### 双方向ネイバー フィルタ リストの管理

バージョン 7.2(1) 以降が稼働する ASA では、このパネルでインターフェイスごとの双方向ネイバー フィルタ リストを定義および管理して、特定のインターフェイスのマルチキャスト送信元アドレスを許可または拒否できます。このパネルのフィールドの詳細については、[\[Add PIM Bidirectional Neighbor Filter\]/\[Edit PIM Bidirectional Neighbor Filter\] ダイアログボックス \(19 ページ\)](#) を参照してください。

### ナビゲーションパス

[Bidirectional Neighbor Filter] タブには、[PIM] ページからアクセスします。詳細については、[PIM の設定 \(14 ページ\)](#) を参照してください。

### 関連項目

- [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#)
- [\[PIM\] ページ - \[Neighbor Filter\] タブ \(17 ページ\)](#)
- [\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#)
- [\[PIM\] ページ - \[Route Tree\] タブ \(23 ページ\)](#)
- [\[PIM\] ページ - \[Request Filter\] タブ \(24 ページ\)](#)

## [Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックス

[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックスは、[\[PIM\] ページ - \[Bidirectional Neighbor Filter\] タブ \(18 ページ\)](#) に表示される双方向ネイバー アクセス コントロール リストでエントリを追加または編集するために使用します。

### ナビゲーションパス

[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックスには、[\[PIM\] ページ - \[Bidirectional Neighbor Filter\] タブ \(18 ページ\)](#) からアクセスできます。

### フィールド リファレンス

表 13: [Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックス

| 要素                   | 説明   |
|----------------------|--|
| インターフェイス (Interface) | この PIM 双方向ネイバーフィルタエントリが適用されるインターフェイスを入力するか、または選択します。 |

| 要素                    | 説明   |
|-----------------------|--|
| Neighbor Filter Group | 選択したアクションが適用される単一のマルチキャストアドレス、またはマルチキャストグループアドレスを入力します。グループアドレス範囲は、標準サブネットマスク（239.0.0.0 255.0.0.0 など）またはCIDRプレフィックス表記法（239.0.0.0/8 など）を使用して入力できます。<br><br>また、指定済みのネットワーク/ホストオブジェクトも選択できます。 |
| 操作                    | 指定したネイバーをDF選択プロセスに参加させるには[許可（permit）]を選択し、指定したネイバーをDF選択プロセスに参加させないためには[拒否（deny）]を選択します。  |

## [PIM] ページ - [Rendezvous Points] タブ

PIMを設定するときは、RPとして動作するルータまたはルーティングデバイスを1つ以上選択する必要があります。RPは、共用配布ツリーの単一の共通ルートであり、デバイスごとにスタティックに設定されます。第1ホップルータは、RPを使用して、送信元のマルチキャストホストに代わって登録パケットを送信します。

複数のグループにサービスを提供するように単一のRPを設定できます。特定のグループを指定していない場合、そのグループのRPはIPマルチキャストグループ範囲（224.0.0.0/4）全体に適用されます。

[Rendezvous Points] パネルは、ランデブーポイントを定義するために使用します。複数のRPを設定できますが、同じRPに複数のエントリは設定できません。

### ナビゲーションパス

[Rendezvous Points] タブには、[PIM] ページからアクセスします。詳細については、[PIMの設定（14ページ）](#)を参照してください。

### 関連項目

- [\[PIM\] ページ - \[Protocol\] タブ（15ページ）](#)
- [\[PIM\] ページ - \[Route Tree\] タブ（23ページ）](#)
- [\[PIM\] ページ - \[Request Filter\] タブ（24ページ）](#)

## フィールドリファレンス

表 14: [Rendezvous Points] タブ

| 要素  | 説明  |
|---|---|
| Generate older IOS compatible register messages | ランデブーポイントが Cisco IOS ルータである場合には、このボックスをオンにします。セキュリティ アプライアンス ソフトウェアが PIM ヘッダーと後続の 4 バイトだけに基づいて計算されたチェックサムを持つ Register メッセージを受け付けるのに対して、Cisco IOS ソフトウェアはすべての PIM メッセージタイプについて、PIM メッセージ全体に基づいて計算されたチェックサムを持つ Register メッセージを受け付けます。 |
| Rendezvous Points table                         | セキュリティ アプライアンスに現在設定されているランデブーポイントを表示します。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、このリストを管理します。[Add Row] および [Edit Row] ボタンを使用すると、 <a href="#">[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス (21 ページ)</a> が開きます。     |

## [Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス

[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックスは、[Rendezvous Points] テーブルにエンTRIESを追加するため、または既存のランデブーポイントエンTRIESを編集するために使用します。次の点に注意してください。

- 同じランデブーポイントアドレスは 2 回使用できません。
- 複数のランデブーポイントに「全グループ」を指定することはできません。

## ナビゲーションパス

[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックスには、[\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#) からアクセスできます。

## フィールドリファレンス

表 15: [Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス

| 要素                          | 説明   |
|-----------------------------|--|
| Rendezvous Point IP Address | ランデブーポイントの IP アドレスを入力します。これはユニキャストアドレスです。また、[Select] をクリックして、ネットワーク/ホストオブジェクトを選択することもできます。<br><br>ランデブーポイントエンTRIESを編集するときには、この値を変更できません。 |

[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス

| 要素   | 説明   |
|--|--|
| Use bi-directional forwarding                                      | <p>指定したマルチキャスト グループを双方向モードで動作させる場合には、このボックスをオンにします。双方向モードでは、セキュリティアプライアンスはマルチキャスト パケットを受信し、自らに直接接続されたメンバーまたは PIM ネイバーが存在しない場合、送信元に Prune メッセージを返します。指定したマルチキャスト グループをスパス モードで動作させる場合には、このボックスをオフにします。</p> <p>(注) セキュリティアプライアンスは、実際の双方向設定に関係なく常に PIM hello メッセージで双方向機能をアドバタイズします。</p>   |
| この RP をすべてのマルチキャストグループに使用する (Use this RP for All Multicast Groups) | <p>インターフェイスのすべてのマルチキャスト グループに、指定されたランデブー ポイントを使用するには、このオプションを選択します。</p>  |
| Use this RP for the Multicast Groups as specified below            | <p>指定のランデブー ポイントを使用するマルチキャスト グループを定義するには、このオプションを選択します。[Multicast Groups] テーブルがアクティブになります。</p>   |
| [Multicast Groups] テーブル  | <p>指定のランデブー ポイントに現在関連付けられているマルチキャスト グループが表示されます。</p> <p>テーブルエントリは上から順に処理されます。たとえば、マルチキャスト グループの範囲を含むエントリを作成してから、その範囲内の特定グループに対する拒否ルールをテーブルの一番上に配置することによって、その特定グループを除外できます。つまり、マルチキャスト グループの範囲に対する許可ルールを、個々の拒否ステートメントの後ろに続けます。</p> <p>テーブルの下部にあるボタンを使用して <a href="#">[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス (22 ページ)</a> を開き、エントリの追加または編集、エントリの削除、およびテーブル内でのエントリの上下移動を行います。</p> |

[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス

[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックスは、[Add/Edit Rendezvous Point] ダイアログボックスに表示される [Multicast Groups] テーブルのマルチキャスト グループルールを作成するため、またはマルチキャストグループルールを変更するために使用します。また、このダイアログボックスは、[Route Tree] タブで [Shared Tree] ルート フィルタリングを使用するマルチキャスト グループを個別に指定する場合にも使用します。

### ナビゲーションパス

ランデブーポイントを定義するときは、[\[Add Rendezvous Point\]/\[Edit Rendezvous Point\] ダイアログボックス \(21 ページ\)](#) から [\[Add Multicast Group Rules\]/\[Edit Multicast Group Rules\] ダイアログボックス](#) にアクセスします。詳細については、[\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#) を参照してください。

PIM Register メッセージのフィルタリング方法を指定するときは、[\[PIM\] ページ - \[Route Tree\] タブ \(23 ページ\)](#) の [\[Multicast Groups\]](#) テーブルの下にある [\[Add Row\]](#) ボタンまたは [\[Edit Row\]](#) ボタンをクリックして、このダイアログボックスを開きます。

### フィールドリファレンス

表 16: [\[Add Multicast Group Rules\]/\[Edit Multicast Group Rules\]](#) ダイアログボックス

| 要素                      | 説明   |
|-------------------------|--|
| 操作                      | 指定したマルチキャストアドレスを許可するグループルールを作成するには、 <a href="#">[許可 (permit)]</a> を選択します。指定したマルチキャストアドレスを拒否するグループルールを作成するには、 <a href="#">[拒否 (deny)]</a> を選択します。 |
| Multicast Group Network | グループに関連付けられたマルチキャストアドレスおよびネットワークマスクを入力するか、または目的のネットワーク/ホストオブジェクトを選択します。  |

## [PIM] ページ - [Route Tree] タブ

セキュリティアプライアンスがランデブーポイントとして機能している場合は、[\[Route Tree\] タブ](#) を使用して、さまざまな送信元からの PIM Register メッセージをどのようにフィルタリングするかを指定します。具体的には、すべてのマルチキャストグループまたは特定のマルチキャストアドレスだけを対象に、最短パスツリーまたは共有ツリーのいずれかを指定します。

### ナビゲーションパス

[\[Route Tree\] タブ](#) には、[\[PIM\] ページ](#) からアクセスできます。詳細については、[PIM の設定 \(14 ページ\)](#) を参照してください。

### 関連項目

- [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#)
- [\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#)
- [\[PIM\] ページ - \[Request Filter\] タブ \(24 ページ\)](#)

## フィールド リファレンス

表 17: [Route Tree] タブ

| 要素   | 説明  |
|--|---|
| If., specify how the PIM register messages from various sources are filtered | <p>ツリー/グループ オプションを選択します。</p> <ul style="list-style-type: none"> <li>• [すべてのグループに最短パスツリーを使用 (Use Shortest Path Tree for All Groups) ]: セキュリティアプライアンスは、すべてのマルチキャストグループに最短パスツリーを使用します。</li> <li>• [すべてのグループに共有ツリーを使用 (Use Shared Tree for All Groups) ]: セキュリティアプライアンスは、すべてのマルチキャストグループに共有ツリーを使用します。</li> <li>• [以下に指定されているグループに共有ツリーを使用 (Use Shared Tree for the Groups specified below) ]: セキュリティアプライアンスは、[マルチキャストグループ (Multicast Groups) ] テーブルの下で指定されているグループに共有ツリーを使用します。[Multicast Groups] テーブルに記載されていないグループには、最短パス ツリーが使用されません。</li> </ul> |
| [Multicast Groups] テーブル  | <p>共有ツリーを使用するマルチキャスト グループが表示されます。</p> <p>テーブル エントリは上から順に処理されます。たとえば、マルチキャスト グループの範囲を含むエントリを作成してから、その範囲内の特定グループに対する拒否ルールをテーブルの一番上に配置することによって、その特定グループを除外できます。つまり、マルチキャスト グループの範囲に対する許可ルールを、個々の拒否ステートメントの後ろに続けます。</p> <p>テーブルの下部にあるボタンを使用して <a href="#">[Add Multicast Group Rules]</a>/<a href="#">[Edit Multicast Group Rules]</a> ダイアログボックス (22 ページ) を開き、エントリの追加または編集、エントリの削除、およびテーブル内でのエントリの上下移動を行います。</p>  |

## [PIM] ページ - [Request Filter] タブ

セキュリティアプライアンスがランデブーポイントとして機能しているときには、ランデブーポイントに登録されるマルチキャスト送信元を制限できます。これにより、未認可の送信元がランデブーポイントに登録されることを回避できます。[Request Filter] タブでは、セキュリティアプライアンスが PIM Register メッセージを受け付けるマルチキャスト送信元と、拒否するマルチキャスト送信元を定義できます。



## ナビゲーションパス

[Request Filter] タブには、[PIM] ページからアクセスできます。詳細については、[PIM の設定 \(14 ページ\)](#) を参照してください。

## 関連項目

- [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#)
- [\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#)
- [\[PIM\] ページ - \[Route Tree\] タブ \(23 ページ\)](#)

## フィールド リファレンス

表 18: [Request Filter] タブ

| 要素   | 説明   |
|--|--|
| 次を使用して PIM Register メッセージをフィルタリング (Filter PIM register messages using) | <p>さまざまなマルチキャストグループを対象に、PIM Register メッセージのフィルタリング方法を選択します。</p> <ul style="list-style-type: none"> <li>• [なし (None) ] : PIM Register メッセージをフィルタリングしません。</li> <li>• [ルートマップ (route-map) ] : 指定のルートマップを使用して、PIM Register メッセージをフィルタリングします。[ルートマップ (Route Map) ] フィールドがアクティブになります。ルート マップで許可される PIM Register メッセージだけが、ランデブーポイントに到達できます。</li> <li>• [アクセスリスト (access-list) ] : アクセスリストを使用して、PIM Register メッセージをフィルタリングします。[マルチキャストグループ (Multicast Groups) ] テーブルがアクティブになります。アクセスリストで許可される PIM Register メッセージだけが、ランデブーポイントに到達できます。</li> </ul> |
| ルート マップ  | <p>フィルタとして [ルートマップ (route-map) ] を選択したときは、ルートマップ名を入力します。参照先のルートマップで標準のホスト ACL を使用します。拡張 ACL はサポートされません。</p> <p>(注) このフィールドにはルートマップ名だけが含まれます。ルートマップは、FlexConfig 内で作成および格納されます。</p>  |

**[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス**

| 要素                      | 説明  |
|-------------------------|---|
| [Multicast Groups] テーブル | <p>マルチキャストグループとして現在定義されている要求フィルタールールを表示します。</p> <p>テーブルエントリは上から順に処理されます。たとえば、マルチキャストグループの範囲を含むエントリを作成してから、その範囲内の特定グループに対する拒否ルールをテーブルの一番上に配置することによって、その特定グループを除外できます。つまり、マルチキャストグループの範囲に対する許可ルールを、個々の拒否ステートメントの後ろに続けます。</p> <p>テーブルの下部にあるボタンを使用して <a href="#">[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス (22 ページ)</a> を開き、エントリの追加または編集、エントリの削除、およびテーブル内でのエントリの上下移動を行います。</p> |

**[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス**

[Add/Edit Multicast Group Rules] ダイアログボックスは、アプライアンスがランデブーポイントとして機能するときに、セキュリティアプライアンスへの登録を拒否または許可するマルチキャスト送信元を定義するために使用します。送信元 IP アドレスおよび宛先マルチキャストアドレスに基づいて、フィルタールールを作成します。

**ナビゲーションパス**

[Add/Edit Multicast Group Rules] ダイアログボックスには、[\[PIM\] ページ - \[Request Filter\] タブ \(24 ページ\)](#) からアクセスできます。

**フィールド リファレンス**

表 19: [\[Add Multicast Group Rules\]/\[Edit Multicast Group Rules\] ダイアログボックス](#)

| 要素        | 説明  |
|-----------|---|
| 操作        | 指定した宛先マルチキャストトラフィックの指定した送信元に対してセキュリティアプライアンスへの登録を許可するルールを作成するには、[許可 (permit)] を選択します。指定した送信元/宛先マルチキャストトラフィックへの登録を拒否するルールを作成するには、[拒否 (deny)] を選択します。 |
| 送信元ネットワーク | Register メッセージ送信元の IP アドレスおよびネットワーク マスクを入力するか、または適切なネットワーク/ホスト オブジェクトを選択します。  |
| 宛先ネットワーク  | マルチキャスト宛先の IP アドレスおよびネットワーク マスクを入力するか、または適切なネットワーク/ホスト オブジェクトを選択します。  |

## PIM ページ - ブートストラップルータ タブ

PIM ブートストラップルータ (BSR) は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント (RP) セレクションモデルです。RP 機能には RP の検出が含まれており、RP にデフォルトルートを提供します。これは、一連のデバイスを BSR の選択プロセスに参加する候補の BSR (C-BSR) として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブーポイント (C-RP) として設定されたデバイスは、選定された BSR にグループマッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経路で、マルチキャストツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

[ブートストラップルータ (Boot Strap Router) ] タブを使用して、デバイスを PIM ブートストラップルータとして設定できます。

### ナビゲーションパス

[PIM] ページから [ブートストラップルータ (Boot Strap Router) ] タブにアクセスできます。詳細については、[PIM の設定 \(14 ページ\)](#) を参照してください。

### 関連項目

- [\[PIM\] ページ - \[Protocol\] タブ \(15 ページ\)](#)
- [\[PIM\] ページ - \[Rendezvous Points\] タブ \(20 ページ\)](#)
- [\[PIM\] ページ - \[Route Tree\] タブ \(23 ページ\)](#)

### フィールドリファレンス

表 20: [ブートストラップルータ (Boot Strap Router) ] タブ

| 要素                   | 説明  |
|----------------------|---|
| インターフェイス (Interface) | BSR アドレスを候補の BSR にするため、アドレスの派生元のインターフェイスを選択します。   |
| ハッシュマスク長             | ハッシュ関数が呼び出される前にグループアドレスと AND 演算されるマスクの長さを入力します。ハッシュ元が同じであるすべてのグループは、同じランデブーポイント (RP) に対応します。<br><br>たとえば、マスク長が 24 の場合、グループアドレスの最初の 24 ビットだけが使用されます。これにより、複数のグループについて 1 つの RP を取得できます。 |
| プライオリティ              | BSR 候補の優先順位を入力します。プライオリティが大きな BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。   |

## [ブートストラップルータの追加/編集 (Add/Edit Bootstrap Router) ] ダイアログボックス

[ブートストラップルータの追加/編集 (Add/Edit Bootstrap Router) ] ダイアログボックスを使用して、ブートストラップルータをボーダー BSR として設定します。BSR メッセージを異なるドメイン間で交換しないでください。そのようにすると、一方のドメインにあるルータが他方のドメインにあるランデブーポイント (RP) を選択し、結果としてドメイン間でプロトコルが誤動作したり分離が行われなかったりする可能性があるためです。

PIM スパースモード (PIM-SM) のドメインの境界インターフェイスは、特にそのインターフェイスによって到達可能な隣接ドメインも PIM-SM を実行している場合、該当するドメインとの特定のトラフィックのやりとりを回避するように設定されています。そのため、該当するインターフェイスでの BSR メッセージの送受信を防ぐ目的で、そのインターフェイスをボーダー BSR として設定します。

### ナビゲーションパス

[ブートストラップルータの追加/編集 (Add/Edit Bootstrap Router) ] ダイアログボックスには、[PIM ページ - ブートストラップルータ タブ \(27 ページ\)](#) からアクセスできます。

### フィールド リファレンス

表 21: [ブートストラップルータの追加/編集] ダイアログボックス

| 要素  | 説明  |
|---|---|
| (任意) [BSR ボーダー (BSR Border) ] テーブルの [追加 (Add) ] | インターフェイスを追加し、ボーダー BSR として設定します。インターフェイスがボーダー BSR として設定されている場合、PIM BSR メッセージは送受信されません。 |

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。