



マルチキャスト ルーティングの設定

マルチキャスト ルーティングは、シングルルーテッド モードでのみサポートされます。ここでは、次の項目について説明します。

- [マルチキャスト \(P. 17-2\)](#) : セキュリティ アプライアンスでのマルチキャスト ルーティングをイネーブルまたはディセーブルにします。
- [IGMP \(P. 17-3\)](#) : セキュリティ アプライアンスで IGMP を設定します。
- [Multicast Route \(P. 17-9\)](#) : スタティック マルチキャスト ルートを定義します。
- [MBoundary \(P. 17-11\)](#) : 管理用に範囲を定めたマルチキャスト アドレスの境界を設定します。
- [MForwarding \(P. 17-13\)](#) : インターフェイスごとのマルチキャスト転送をイネーブルまたはディセーブルにします。
- [PIM \(P. 17-14\)](#) : セキュリティ アプライアンスで PIM を設定します。

マルチキャスト

Multicast ペインでは、セキュリティ アプライアンスでのマルチキャスト ルーティングをイネーブルにできます。

マルチキャスト ルーティングをイネーブルにすることで、デフォルトですべてのインターフェイス上の IGMP および PIM がイネーブルになります。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認識するために使用します。ホストは、IGMP レポート メッセージを送信してマルチキャスト 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転送テーブルを維持します。



(注)

マルチキャスト ルーティングでサポートされているのは UDP トランスポート レイヤのみです。

フィールド

Enable Multicast Routing : セキュリティ アプライアンスでの IP マルチキャスト ルーティングをイネーブルにするには、このチェックボックスをオンにします。IP マルチキャスト ルーティングをディセーブルにするには、このチェックボックスをオフにします。デフォルトでは、マルチキャストはディセーブルになっています。マルチキャストをイネーブルにすると、すべてのインターフェイス上でマルチキャストがイネーブルになります。マルチキャストはインターフェイスごとにディセーブルにできます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	—	•	—	—

詳細情報

[マルチキャスト ルーティングの設定 \(P. 17-1\)](#)

[IGMP \(P. 17-3\)](#)

[Multicast Route \(P. 17-9\)](#)

[MBoundary \(P. 17-11\)](#)

[MForwarding \(P. 17-13\)](#)

[PIM \(P. 17-14\)](#)

IGMP

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP はグループ アドレス (クラス D IP アドレス) を使用します。ホスト グループ アドレスは、224.0.0.0 ~ 239.255.255.255 の範囲で使用できます。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。

セキュリティ アプライアンスでの IGMP の設定の詳細については、次の項目を参照してください。

- [Access Group](#)
- [Join Group](#)
- [Protocol](#)
- [Static Group](#)

Access Group

アクセス グループは、インターフェイス上で許可されるマルチキャスト グループを制御します。

フィールド

- **Access Groups** : 各インターフェイスに定義されたアクセス グループを表示します。
テーブル エントリは、上から下の順で処理されます。具体的なエントリはテーブルの上方に、一般的なエントリは下方に配置してください。たとえば、特定のマルチキャスト グループを許可するアクセス グループ エントリはテーブルの上方に配置し、許可ルールにあるグループを含むマルチキャスト グループの範囲を拒否するアクセス グループ エントリは下方に配置します。そのグループは、拒否ルールの前に許可ルールが強制されるため、許可されます。
テーブルのエントリをダブルクリックすると、選択したエントリを対象とした [Add/Edit Access Group](#) ダイアログボックスが開きます。
 - **Interface** : アクセス グループが関連付けられたインターフェイスを表示します。
 - **Action** : アクセス ルールでマルチキャスト グループ アドレスが許可される場合、「Permit」を表示します。アクセス ルールでマルチキャスト グループ アドレスが拒否される場合は「Deny」を表示します。
 - **Multicast Group Address** : アクセス ルールが適用されるマルチキャスト グループ アドレスを表示します。
 - **Netmask** : マルチキャスト グループ アドレスのネットワーク マスクを表示します。
- **Insert Before** : [Add/Edit Access Group](#) ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいアクセス グループ エントリを追加するには、このボタンを使用します。
- **Insert After** : [Add/Edit Access Group](#) ダイアログボックスが開きます。テーブルで選択したエントリの後に新しいアクセス グループ エントリを追加するには、このボタンを使用します。
- **Add** : [Add/Edit Access Group](#) ダイアログボックスが開きます。テーブルの一番下に新しいアクセス グループ エントリを追加するには、このボタンを使用します。
- **Edit** : [Add/Edit Access Group](#) ダイアログボックスが開きます。選択したアクセス グループ エントリの情報を変更するには、このボタンを使用します。
- **Delete** : 選択したアクセス グループ エントリをテーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit Access Group

Add Access Group ダイアログボックスでは、新しいアクセス グループを Access Group テーブルに追加できます。Edit Access Group ダイアログボックスでは、既存のアクセス グループ エントリの情報を変更できます。既存のエントリを編集するとき、一部のフィールドはブロックされていることがあります。

フィールド

- Interface : アクセス グループが関連付けられたインターフェイスを選択します。既存のアクセス グループを編集するときは、関連インターフェイスを変更できません。
- Action : 選択した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には「permit」を選択します。選択したインターフェイスからマルチキャスト グループをフィルタリングするには「deny」を選択します。
- Multicast Group Address : アクセス グループが適用されるマルチキャスト グループのアドレスを入力します。
- Netmask : マルチキャスト グループ アドレスのネットワーク マスクを入力するか、リストから共通ネットワーク マスクの 1 つを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Join Group

セキュリティ アプライアンスをマルチキャスト グループのメンバーとして設定できます。Join Group ペインでは、セキュリティ アプライアンスがメンバーになっているマルチキャスト グループを表示します。



(注)

特定のグループのマルチキャスト パケットを、セキュリティ アプライアンスにグループの一部として受け入れさせずにインターフェイスに転送する場合は、「[Static Group](#)」を参照してください。

フィールド

- Join Group : 各インターフェイスのマルチキャストグループメンバーシップを表示します。
 - Interface : セキュリティ アプライアンス インターフェイスの名前を表示します。
 - Multicast Group Address : インターフェイスの属するマルチキャストグループのアドレスを表示します。
- Add : [Add/Edit IGMP Join Group](#) ダイアログボックスが開きます。インターフェイスに新しいマルチキャストグループメンバーシップを追加するには、このボタンを使用します。
- Edit : [Add/Edit IGMP Join Group](#) ダイアログボックスが開きます。既存のマルチキャストグループメンバーシップエントリを編集するには、このボタンを使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit IGMP Join Group

インターフェイスをマルチキャストグループのメンバーに設定するには、Add IGMP Join Group ダイアログボックスを使用します。既存のメンバーシップ情報を変更するには、Edit IGMP Join Group ダイアログボックスを使用します。

フィールド

- Interface : マルチキャストグループメンバーシップを設定するセキュリティ アプライアンス インターフェイスの名前を選択します。既存のエントリを編集している場合、この値は変更できません。
- Multicast Group Address : このフィールドにマルチキャストグループのアドレスを入力します。グループアドレスは 224.0.0.0 ~ 239.255.255.255 で入力する必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Protocol

Protocol ペインでは、セキュリティ アプライアンス上の各インターフェイスの IGMP パラメータを表示します。

フィールド

- Protocol : 各インターフェイスに設定された IGMP パラメータを表示します。このテーブルの行をダブルクリックすると、選択したインターフェイスを対象とした [Configure IGMP Parameters](#) ダイアログボックスが開きます。

- Interface : インターフェイスの名前を表示します。
- Enabled : IGMP がインターフェイス上でイネーブルになっている場合は、「Yes」を表示します。IGMP がインターフェイス上でディセーブルになっている場合は、「No」を表示します。
- Version : インターフェイス上でイネーブルになっている IGMP のバージョンを表示します。
- Query Interval : 指定したルータが IGMP ホストクエリーメッセージを送信する間隔を秒数で表示します。
- Query Timeout : 前のクエリアが引き継ぎを停止した後で、セキュリティアプライアンスがインターフェイスのクエリアとして引き継ぐまでの期間を表示します。
- Response Time : IGMP クエリーでアドバタイズされる最大応答時間を秒数で表示します。この設定への変更は、IGMP バージョン 2 に対してのみ有効です。
- Group Limit : インターフェイスで許可される最大グループ数を表示します。
- Forward Interface : 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を表示します。
- Edit : 選択したインターフェイスを対象とした [Configure IGMP Parameters](#) ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Configure IGMP Parameters

Configure IGMP Parameters ダイアログボックスでは、IGMP をディセーブルにして、選択したインターフェイス上の IGMP パラメータを変更できます。

フィールド

- Interface : 設定しているインターフェイスの名前を表示します。このフィールドに表示される情報は変更できません。
- Enable IGMP : インターフェイスで IGMP をイネーブルにするには、このチェックボックスをオンにします。インターフェイスで IGMP をディセーブルにするには、このチェックボックスをオフにします。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した場合、IGMP はデフォルトでイネーブルになっています。
- Version : インターフェイスでイネーブルにする IGMP のバージョンを選択します。IGMP バージョン 1 をイネーブルにするには 1 を、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。一部の機能では、IGMP バージョン 2 が必要になります。デフォルトでは、セキュリティアプライアンスは IGMP バージョン 2 を使用します。
- Query Interval : 指定したルータが IGMP ホストクエリーメッセージを送信する間隔を秒数で入力します。有効値の範囲は 1 ~ 3600 秒です。デフォルト値は、125 秒です。
- Query Timeout : 前のクエリアが引き継ぎを停止した後で、セキュリティアプライアンスがインターフェイスのクエリアとして引き継ぐまでの期間を秒数で入力します。有効値の範囲は 60 ~ 300 秒です。デフォルト値は、255 秒です。

- **Response Time** : IGMP クエリーでアドバタイズされる最大応答時間を秒数で入力します。指定した応答時間内にセキュリティ アプライアンスがホスト レポートを受信しない場合、IGMP グループはプルーニングされます。この値を少なくすると、セキュリティ アプライアンスがグループをプルーニングするのが速くなります。有効値の範囲は 1 ～ 12 秒です。デフォルト値は、10 秒です。この値への変更は、IGMP バージョン 2 に対してのみ有効です。
- **Group Limit** : インターフェイス上で加入する最大ホスト数を入力します。有効値の範囲は 1 ～ 500 です。デフォルト値は 500 です。
- **Forward Interface** : IGMP ホスト レポートの送信先となるインターフェイスの名前を選択します。ホスト レポートの転送をディセーブルにするには「None」を選択します。デフォルトでは、ホスト レポートは転送されません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Static Group

一部の場合では、IGMP クエリーへの応答を防ぐコンフィギュレーションがネットワーク上のホストに設定されていることがあります。それでもマルチキャスト トラフィックをそのネットワーク セグメントに転送するとします。その場合、マルチキャスト トラフィックをネットワーク セグメントに届ける方法は 2 つあります。

- **Join Group** ペインを使用して、インターフェイスをマルチキャスト グループのメンバーとして設定します。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 パケットを指定したインターフェイスに転送するだけでなく、そのパケットを受け入れます。
- **Static Group** ペインを使用して、セキュリティ アプライアンスを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設定します。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を受け取ることはなく、転送だけです。したがって、この方法では高速スイッチングが実現できます。発信インターフェイスが IGMP キャッシュに表示されますが、そのインターフェイス自身はマルチキャスト グループのメンバーではありません。

フィールド

- **Static Group** : 各インターフェイスの、スタティックに割り当てられたマルチキャスト グループを表示します。
 - **Interface** : セキュリティ アプライアンス インターフェイスの名前を表示します。
 - **Multicast Group Address** : インターフェイスに割り当てられたマルチキャスト グループのアドレスを表示します。
- **Add** : [Add/Edit IGMP Static Group](#) ダイアログボックスが開きます。インターフェイスに新しいスタティック グループを追加するには、このボタンを使用します。
- **Edit** : [Add/Edit IGMP Static Group](#) ダイアログボックスが開きます。既存のスタティック グループ メンバーシップを編集するには、このボタンを使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit IGMP Static Group

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には、Add IGMP Static Group ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更するには、Edit IGMP Static Group ダイアログボックスを使用します。

フィールド

- **Interface** : マルチキャスト グループを設定するセキュリティ アプライアンス インターフェイスの名前を選択します。既存のエントリを編集している場合、この値は変更できません。
- **Multicast Group Address** : このフィールドにマルチキャスト グループのアドレスを入力します。グループアドレスは 224.0.0.0 ~ 239.255.255.255 で入力する必要があります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Multicast Route

スタティック マルチキャスト ルートを定義すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、発信元と宛先の間のパスがマルチキャスト ルーティングをサポートしていない場合、2 つのマルチキャスト デバイス間に GRE トンネルを設定し、そのトンネルを経由してマルチキャスト パケットを送信することが解決策となります。

スタティック マルチキャスト ルートは、セキュリティ アプライアンスに対してローカルであり、アドバタイズまたは再配布されることはありません。

フィールド

- **Multicast Route** : セキュリティ アプライアンスでスタティックに定義されたマルチキャスト ルートを表示します。テーブルのエントリをダブルクリックすると、そのエントリを対象とした **Add/Edit Multicast Route** ダイアログボックスが開きます。
 - **Source Address** : マルチキャストの発信元の IP アドレスとマスクを CIDR 表記で表示します。
 - **Source Interface** : マルチキャスト ルートの着信インターフェイスを表示します。
 - **Destination Interface** : マルチキャスト ルートの発信インターフェイスを表示します。
 - **Admin Distance** : スタティック マルチキャスト ルートの管理ディスタンスを表示します。
- **Add** : **Add/Edit Multicast Route** ダイアログボックスが開きます。新しいスタティック ルートを追加するには、このボタンを使用します。
- **Edit** : **Add/Edit Multicast Route** ダイアログボックスが開きます。選択したスタティック マルチキャスト ルートを変更するには、このボタンを使用します。
- **Delete** : 選択したスタティック ルートを削除するには、このボタンを使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit Multicast Route

新しいスタティック 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には、**Add Multicast Route** ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更するには、**Edit Multicast Route** ダイアログボックスを使用します。

フィールド

- **Source Address** : マルチキャストの発信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値を変更できません。
- **Source Mask** : マルチキャストの発信元の IP アドレスのネットワーク マスクを入力するか、リストから共通マスクを選択します。既存のスタティック マルチキャスト ルートを編集しているときは、この値を変更できません。
- **Source Interface** : マルチキャスト ルートの着信インターフェイスを選択します。
- **Destination Interface** : (オプション) マルチキャスト ルートの発信インターフェイスを選択します。宛先インターフェイスを指定した場合、選択したインターフェイスを介してルートが転送されます。宛先インターフェイスを選択しない場合、ルートの転送には RPF が使用されます。

- **Admin Distance** : スタティック マルチキャスト ルートの管理ディスタンスを入力します。スタティック マルチキャスト ルートの管理ディスタンスがユニキャスト ルートの管理ディスタンスと同じ場合、スタティック マルチキャスト ルートが優先されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

MBoundary

MBoundary ペインでは、管理用に範囲を定めたマルチキャストアドレスのマルチキャスト境界を設定できます。マルチキャスト境界は、マルチキャスト データ パケットのフローを制限し、同じマルチキャスト グループ アドレスの異なる管理ドメインでの再使用をイネーブルにします。インターフェイスでマルチキャスト境界が定義されるとき、フィルタ ACL に許可されたマルチキャストトラフィックだけがインターフェイスを通過します。

フィールド

Multicast Boundary テーブルには、次の情報が含まれています。テーブル エントリをダブルクリックすると、マルチキャスト境界のフィルタ設定を編集できます。

- **Interface** : デバイス上のインターフェイスを一覧表示します。
- **Boundary Filter** : 指定したインターフェイスの境界フィルタ エントリを一覧表示します。インターフェイスにマルチキャスト境界が定義されていない場合、このカラムではインターフェイスに「No Boundary Filters Configured」が表示されます。
- **AutoFilter** : Auto-RP メッセージが境界 ACL で拒否されたかどうかが表示されます。AutoFilter がイネーブルになっている場合、ACL では Auto-RP メッセージのフローも制限されます。AutoFilter がディセーブルになっている場合は、すべての Auto-RP メッセージがインターフェイスを通過します。この機能はデフォルトでディセーブルになっています。

Boundary テーブルのエントリでは、次のアクションを実行できます。

- **Edit** : Edit Boundary Filter ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	—	•	—	—

Edit Boundary Filter

Edit Boundary Filter ダイアログボックスでは、マルチキャスト境界フィルタ ACL を表示します。このダイアログボックスを使用して、境界フィルタ ACL エントリを追加および削除できます。

境界フィルタのコンフィギュレーションがセキュリティ アプライアンスに適用されるとき、実行中のコンフィギュレーションには、*interface-name_multicast* という名前の ACL が表示されます。ここで *interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。その名前の ACL がすでに存在する場合、*inside_multicast_1* というように、名前の後ろに番号が付加されます。

フィールド

- **Interface** : マルチキャスト境界フィルタ ACL の設定先に行っているインターフェイスを表示します。
- **Remove any Auto-RP group range** : 境界 ACL で拒否された発信元からの Auto-RP メッセージをフィルタリングするには、このチェックボックスをオンにします。チェックボックスをオフにした場合、すべての Auto-RP メッセージが通過します。

Boundary Filter テーブルには、次の情報が含まれています。

- **Action** : フィルタ エントリのアクションです。Permit では、指定したトラフィックの通過を許可します。Deny では、指定したトラフィックによるインターフェイスの通過を拒否します。インターフェイスでマルチキャスト境界フィルタが設定されるとき、マルチキャストトラフィックはデフォルトで拒否されます。
- **Network Address** : 許可されるまたは拒否されるグループのマルチキャスト グループ アドレスです。
- **Netmask** : マルチキャスト グループアドレスに適用されるネットワーク マスクです。

Boundary Filter テーブルでは次のアクションを実行できます。

- **Insert** : 選択したエントリの前にネイバー フィルタ エントリを挿入します。
- **Add** : 選択したエントリの後ろにネイバー フィルタ エントリを追加します。
- **Edit** : 選択した境界フィルタを編集します。
- **Delete** : 選択したネイバー フィルタ エントリを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit/Insert Neighbor Filter Entry

Add/Edit/Insert Neighbor Filter Entry ダイアログボックスでは、マルチキャスト境界 ACL の ACL エントリを作成できます。

フィールド

- **Action** : ネイバー フィルタ ACL エントリに対して Permit または Deny を選択します。Permit を選択すると、インターフェイスを介したマルチキャスト グループのアドバタイズメントが許可されます。Deny を選択すると、指定したマルチキャスト グループ アドバタイズメントによるインターフェイスの通過を拒否します。インターフェイスでマルチキャスト境界を設定するとき、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャストトラフィックによるインターフェイスの通過が拒否されます。
- **Multicast Group Address** : 許可されるまたは拒否されるマルチキャスト グループのアドレスを入力します。有効なグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。
- **Netmask** : マルチキャスト グループアドレスのネットマスクを入力または選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

MForwarding

MForwarding ペインでは、インターフェイスごとにマルチキャスト転送をディセーブル化および再イネーブル化できます。デフォルトでは、すべてのインターフェイスでマルチキャスト転送がイネーブルになっています。

インターフェイスでマルチキャスト転送がディセーブルになると、他の方法で特に設定されていない限り、インターフェイスはマルチキャスト パケットを受け入れません。また、IGMP パケットは、マルチキャスト転送がディセーブルになっているときも拒否されます。

フィールド

- Multicast Forwarding テーブルには、次の情報が表示されます。
 - **Interface** : セキュリティ アプライアンスで設定されたインターフェイスを表示します。インターフェイスを選択するには、インターフェイス名をクリックします。インターフェイス名をダブルクリックすると、インターフェイスの Multicast Forwarding Enabled ステータスが切り替わります。
 - **Multicast Forwarding Enabled** : 指定したインターフェイスでマルチキャスト転送がイネーブルになっている場合は Yes を表示します。指定したインターフェイスでマルチキャスト転送がディセーブルになっている場合は No を表示します。このエントリをダブルクリックすると、選択したインターフェイスの Yes と No が切り替わります。
- **Enable** : 選択したインターフェイスでのマルチキャスト転送をイネーブルにします。
- **Disable** : 選択したインターフェイスでのマルチキャスト転送をディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

詳細情報

- [マルチキャストルーティングの設定 \(P. 17-1\)](#)

PIM

ルータは、PIM を使用してマルチキャストデータグラムを転送する転送テーブルを維持します。

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き、PIM はデフォルトですべてのインターフェイスでイネーブルになります。PIM はインターフェイスごとにディセーブルにできます。

PIM の設定の詳細については、次の項目を参照してください。

- [Protocol](#)
- [Neighbor Filter \(P. 17-15\)](#)
- [Bidirectional Neighbor Filter \(P. 17-17\)](#)
- [Rendezvous Points](#)
- [Route Tree](#)
- [Request Filter](#)

Protocol

Protocol ペインでは、インターフェイス固有の PIM プロパティが表示されます。

フィールド

- **Protocol** : 各インターフェイスの PIM 設定を表示します。テーブルのエントリをダブルクリックすると、そのエントリを対象とした [Edit PIM Protocol](#) ダイアログボックスが開きます。
 - **Interface** : セキュリティ アプライアンス インターフェイスの名前を表示します。
 - **PIM Enabled** : インターフェイスで PIM がイネーブルになっている場合は「Yes」を、イネーブルになっていない場合は「No」を表示します。
 - **DR Priority** : インターフェイスの優先度を表示します。
 - **Hello Interval** : インターフェイスが PIM の hello メッセージを送信する頻度を秒数で表示します。
 - **Join-Prune Interval** : インターフェイスが PIM の加入およびプルーンング アドバタイズメントを送信する頻度を秒数で表示します。
- **Edit** : 選択したエントリを対象とした [Edit PIM Protocol](#) ダイアログボックスが開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Edit PIM Protocol

Edit PIM Protocol ダイアログボックスでは、選択したインターフェイスの PIM プロパティを変更できます。

フィールド

- **Interface:** 表示のみ。選択したインターフェイスの名前を表示します。この値は編集できません。
- **PIM Enabled:** 選択したインターフェイスで PIM をイネーブルにするには、このチェックボックスをオンにします。選択したインターフェイスで PIM をディセーブルにするには、このチェックボックスをオフにします。
- **DR Priority:** 選択したインターフェイスの指定ルータの優先順位を設定します。サブネットで高い DR 優先順位を持つルータは、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 優先順位は 1 です。この値を 0 に設定すると、適切でないセキュリティアプライアンス インターフェイスがデフォルト ルータになります。
- **Hello Interval:** インターフェイスが PIM hello メッセージを送信する頻度を秒数で入力します。有効値の範囲は 1 ~ 3600 秒です。デフォルト値は、30 秒です。
- **Join-Prune Interval:** インターフェイスが PIM 加入およびプルーンング アドバタイズメントを送信する頻度を秒数で入力します。有効値の範囲は 10 ~ 600 秒です。デフォルト値は、60 秒です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Neighbor Filter

Neighbor Filter ペインでは、セキュリティ アプライアンスで設定された PIM ネイバー フィルタがあれば、その PIM ネイバー フィルタが表示されます。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 ACL です。インターフェイスにネイバー 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、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 アプライアンスでの PIM に参加できます。

PIM ネイバー フィルタのコンフィギュレーションがセキュリティ アプライアンスに適用されるとき、実行中のコンフィギュレーションには、*interface-name_multicast* という名前の ACL が表示されます。ここで *interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。その名前の ACL がすでに存在する場合、*inside_multicast_1* というように、名前の後ろに番号が付加されます。この ACL は、どのデバイスがセキュリティ アプライアンスの PIM ネイバーになれるのかを定義します。

フィールド

PIM Neighbor Filter テーブルには、次の情報が表示されます。テーブルのエントリをダブルクリックすると、選択したエントリを対象とした Edit Neighbor Filter Entry ダイアログボックスが開きます。

- **Interface:** 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の名前を表示します。
- **Action:** 指定したネイバーが PIM に参加できる場合、「permit」を表示します。指定したネイバーが PIM に参加できない場合は「deny」を表示します。
- **Network Address:** 許可または拒否されるネイバーのネットワーク アドレスです。

- Netmask : Network Address と共に使用するネットワーク マスクです。

次のアクションを実行できます。

- Insert : 選択したエントリの前にネイバー フィルタ エントリを挿入します。
- Add : 選択したエントリの後ろにネイバー フィルタ エントリを追加します。
- Edit : 選択したネイバー フィルタ エントリを編集できます。
- Delete : 選択したネイバー フィルタ エントリを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

詳細情報

[Add/Edit/Insert Neighbor Filter Entry \(P. 17-16\)](#)

Add/Edit/Insert Neighbor Filter Entry

Add/Edit/Insert Neighbor Filter Entry では、PIM ネイバー フィルタ ACL の ACL エントリを作成できます。

フィールド

- Interface : 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の名前をリストから選択します。
- Action : 「permit」を選択すると、指定したネイバーが PIM に参加できます。「deny」を選択すると、指定したネイバーは PIM に参加できません。
- Network Address : 許可または拒否されるネイバーのネットワーク アドレスです。
- Netmask : Network Address と共に使用するネットワーク マスクです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Bidirectional Neighbor Filter

Bidirectional Neighbor Filter ペインでは、セキュリティ アプライアンスで設定された PIM 双方向ネイバー フィルタがあれば、その PIM 双方向ネイバー フィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。インターフェイスに PIM 双方向ネイバー フィルタが設定されていない場合、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合、ACL で許可されるネイバーだけが DF 選定プロセスに参加できます。

PIM 双方向ネイバー フィルタのコンフィギュレーションがセキュリティ アプライアンスに適用されると、実行中のコンフィギュレーションには、*interface-name_multicast* という名前の ACL が表示されます。ここで *interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。その名前の ACL がすでに存在する場合、*inside_multicast_1* というように、名前の後ろに番号が付加されます。この ACL は、どのデバイスがセキュリティ アプライアンスの PIM ネイバーになれるのかを定義します。

双方向 PIM により、マルチキャスト ルータは減少したステート情報を維持できます。セグメント内のすべてのマルチキャスト ルータは、双方向ルータが DF を選定できるように、双方向にイネーブル化されている必要があります。

PIM 双方向ネイバー フィルタは、DF 選定に参加するルータを指定することにより、希薄モード専用から双方向ネットワークへの移行をイネーブルにします。すべてのルータは、そのまま希薄モード ドメインにも参加できます。双方向にイネーブル化された各ルータは、セグメントに非双方向ルータがある場合でも、それぞれのルータの中から DF を選定することができます。非双方向ルータ上のマルチキャスト境界は、双方向グループからの PIM メッセージやデータが双方向サブセット クラウドを出入りしないように防ぎます。

PIM 双方向ネイバー フィルタがイネーブルになると、ACL が許可するルータは双方向機能があると見なされます。したがって、次のような結果になります。

- 許可されたネイバーが双方向をサポートしていない場合、DF 選定は行われません。
- 拒否されたネイバーが双方向をサポートしている場合、DF 選定は行われません。
- 拒否されたネイバーが双方向をサポートしていない場合、DF 選定が行われることがあります。

フィールド

PIM Bidirectional Neighbor Filter テーブルには、次のエントリが含まれています。エントリをダブルクリックすると、そのエントリを対象とした Edit Bidirectional Neighbor Filter Entry ダイアログボックスが開きます。

- **Interface** : 双方向ネイバー フィルタが適用されるインターフェイスを表示します。
- **Action** : 双方向ネイバー フィルタが DF 選定プロセスへの参加を許可する場合、「permit」を表示します。エントリにより、指定したアドレスが DF 選定プロセスに参加できない場合は「deny」を表示します。
- **Network Address** : 許可または拒否されるアドレスです。
- **Netmask** : Network Address に適用されるネットワーク マスクです。

次のアクションを実行できます。

- **Insert** : 選択したエントリの前に双方向ネイバー フィルタ エントリを挿入します。
- **Add** : 選択したエントリの後ろに双方向ネイバー フィルタ エントリを追加します。
- **Edit** : 選択した双方向ネイバー フィルタ エントリを編集できます。
- **Delete** : 選択した双方向ネイバー フィルタ エントリを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

詳細情報

[Add/Edit/Insert Bidirectional Neighbor Filter Entry \(P. 17-18\)](#)

Add/Edit/Insert Bidirectional Neighbor Filter Entry

Add/Edit/Insert Bidirectional Neighbor Filter Entry ダイアログボックスでは、PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成できます。

フィールド

- Interface : PIM 双方向ネイバー フィルタ ACL エントリを設定するインターフェイスを選択します。
- Action : 指定したデバイスが DF 選定に参加できるようにするには **permit** を選択します。指定したデバイスが DF 選定に参加できないようにするには **deny** を選択します。
- Network Address : 許可または拒否されるネイバーのネットワーク アドレスです。
- Netmask : Network Address と共に使用するネットワーク マスクです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Rendezvous Points

PIM を設定するとき、RP として動作するルータを 1 つ以上選択する必要があります。RP は、共有配布ツリーの単一で共通のルートで、各ルータでスタティックに設定されます。最初のホップルータは、RP を使用し、発信元マルチキャスト ホストの代わりに登録パケットを送信します。

1 つの RP が複数のグループに機能するように設定できます。特定のグループが指定されていない場合は、IP マルチキャスト グループ全体の範囲 (224.0.0.0/4) にグループの RP が適用されます。

複数の RP を設定できますが、同じ RP 内で保持できるエントリは 1 つです。

フィールド

- Generate IOS compatible register messages : RP が Cisco IOS ルータの場合、このチェックボックスをオンにします。セキュリティ アプライアンス ソフトウェアは、Cisco IOS ソフトウェア方式 (すべての PIM メッセージ タイプの PIM メッセージ全体のチェックサムと共に登録メッセージを受け入れる方法) ではなく、PIM ヘッダーにあるチェックサムおよび次の 4 バイトのみと共に登録メッセージを受け入れます。

- Rendezvous Points : セキュリティ アプライアンスで設定された RP を表示します。
 - Rendezvous Point : RP の IP アドレスを表示します。
 - Multicast Groups : RP に関連付けられたマルチキャスト グループを表示します。RP がインターフェイス上のすべてのマルチキャスト グループに関連付けられている場合は、「--All Groups--」を表示します。
 - Bi-directional : 指定したマルチキャスト グループが双方向モードで動作する場合は、「Yes」を表示します。指定したグループが希薄モードで動作する場合は、「No」を表示します。
- Add : [Add/Edit Rendezvous Point](#) ダイアログボックスが開きます。新しい RP エントリを追加するには、このボタンを使用します。
- Edit : [Add/Edit Rendezvous Point](#) ダイアログボックスが開きます。既存の RP エントリを変更するには、このボタンを使用します。
- Delete : 選択した RP エントリを Rendezvous Point テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit Rendezvous Point

Add Rendezvous Point ダイアログボックスでは、新しいエンタリを Rendezvous Point テーブルに追加できます。Edit Rendezvous Point ダイアログボックスでは、既存の RP エントリを変更できます。

制約事項

- 同じ RP アドレスを 2 回使用することはできません。
- 複数の RP に All Groups を指定することはできません。

フィールド

- Rendezvous Point IP Address : RP 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。既存の RP エントリを編集するときは、この値を変更できません。
- Use bi-directional forwarding : 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は、このチェック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 アプライアンスがマルチキャスト パケットを受信し、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、送信元にルーティング メッセージを戻します。指定したマルチキャスト グループを希薄モードで動作させる場合は、このチェックボックスをオフにします。



(注) セキュリティ アプライアンスは、実際の双方向構成にかかわらず、PIM の hello メッセージを使用して双方向の機能を常時アドバタイズします。

- Use this RP for All Multicast Groups : インターフェイス上のすべてのマルチキャスト グループの指定した RP を使用するには、このオプションを選択します。
- Use this RP for the Multicast Groups as specified below : マルチキャスト グループを指定した RP で使用するよう指定するには、このオプションを選択します。

- **Multicast Groups** : 指定した RP に関連付けられたマルチキャスト グループを表示します。
 テーブル エントリは、上から下の順で処理されます。特定のグループの拒否ルールをテーブルの一番上に、マルチキャスト グループの範囲の許可ルールを deny 文の下にそれぞれ配置すれば、マルチキャスト グループの範囲を含みながらその範囲内の特定グループを除外する RP エントリを作成できます。
 エントリをダブルクリックすると、選択したエントリを対象とした **Multicast Group** ダイアログボックスが開きます。
 - **Action** : マルチキャスト グループが含まれる場合は「Permit」を、マルチキャスト グループが除外される場合は「deny」を表示します。
 - **Multicast Group Address** : マルチキャスト グループのアドレスを表示します。
 - **Netmask** : マルチキャスト グループアドレスのネットワーク マスクを表示します。
- **Insert Before** : **Multicast Group** ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- **Insert After** : **Multicast Group** ダイアログボックスが開きます。テーブルで選択したエントリの後に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- **Add** : **Multicast Group** ダイアログボックスが開きます。テーブルの一番下に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- **Edit** : **Multicast Group** ダイアログボックスが開きます。選択したマルチキャスト グループ エントリの情報を変更するには、このボタンを使用します。
- **Delete** : 選択したマルチキャスト グループ エントリをテーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	—	•	—	—

Multicast Group

マルチキャスト グループとは、どのマルチキャスト アドレスがグループの一部であるかを定義するアクセス ルールのリストです。マルチキャスト グループには、1 つのマルチキャスト アドレスまたはマルチキャスト アドレスの範囲を含めることができます。新しいマルチキャスト グループ ルールを作成するには、**Add Multicast Group** ダイアログボックスを使用します。既存のマルチキャスト グループ ルールを変更するには、**Edit Multicast Group** ダイアログボックスを使用します。

フィールド

- **Action** : 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、「Permit」を選択します。指定したマルチキャスト アドレスをフィルタリングするグループ ルールを作成するには、「Deny」を選択します。
- **Multicast Group Address** : グループに関連付けられたマルチキャスト アドレスを入力します。
- **Netmask** : マルチキャスト グループアドレスのネットワーク マスクを入力または選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Request Filter

セキュリティ アプライアンスが RP として動作しているとき、特定のマルチキャスト送信元の登録を制限できます。この制限により、認可されない送信元が RP で登録されなくなります。Request Filter ペインでは、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入れるマルチキャストの送信元を定義できます。

フィールド

- **Multicast Groups** : 要求フィルタ アクセスルールを表示します。

テーブル エントリは、上から下の順で処理されます。特定のグループの拒否ルールをテーブルの一番上に、マルチキャスト グループの範囲の許可ルールを deny 文の下にそれぞれ配置すれば、マルチキャスト グループの範囲を含みながらその範囲内の特定グループを除外するエントリを作成できます。

エントリをダブルクリックすると、選択したエントリを対象とした **Request Filter Entry** ダイアログボックスが開きます。

- **Action** : マルチキャストの送信元による登録が許可される場合は「Permit」を、マルチキャストの送信元が除外される場合は「deny」を表示します。
- **Source** : 登録メッセージの送信元のアドレスを表示します。
- **Destination** : マルチキャストの宛先アドレスを表示します。
- **Insert Before** : **Request Filter Entry** ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- **Insert After** : **Request Filter Entry** ダイアログボックスが開きます。テーブルで選択したエントリの後に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- **Add** : **Request Filter Entry** ダイアログボックスが開きます。テーブルの一番下に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- **Edit** : **Request Filter Entry** ダイアログボックスが開きます。選択したマルチキャスト グループ エントリの情報を変更するには、このボタンを使用します。
- **Delete** : 選択したマルチキャスト グループ エントリをテーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Request Filter Entry

Request Filter Entry ダイアログボックスでは、セキュリティ アプライアンスが RP として動作するときにはマルチキャストの送信元がセキュリティ アプライアンスで登録できるように定義します。フィルタ ルールは、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作成します。

フィールド

- **Action** : 指定したマルチキャスト トラフィックの指定送信元によるセキュリティ アプライアンスでの登録を許可するルールを作成するには「Permit」を選択します。指定したマルチキャスト トラフィックの指定送信元によるセキュリティ アプライアンスでの登録を許可しないルールを作成する場合は「Deny」を選択します。
- **Source IP Address** : 登録メッセージの送信元の IP アドレスを入力します。
- **Source Netmask** : 登録メッセージの送信元のネットワーク マスクを入力または選択します。
- **Destination IP Address** : マルチキャスト宛先アドレスを入力します。
- **Destination Netmask** : マルチキャスト宛先アドレスのネットワーク マスクを入力または選択します。

モード

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	—	•	—	—

Route Tree

デフォルトでは、PIM リーフ ルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。この加入によって遅延は少なくなります。共有ツリーより多くのメモリが必要となります。

すべてのマルチキャスト グループに対して、または特定のマルチキャスト アドレスに対して、セキュリティ アプライアンスが最短パス ツリーに加入するか、共有ツリーを使用するかを設定できます。

フィールド

- **Use Shortest Path Tree for All Groups** : すべてのマルチキャスト グループに最短パス ツリーを使用するには、このオプションを選択します。
- **Use Shared Tree for All Groups** : すべてのマルチキャスト グループに共有ツリーを使用するには、このオプションを選択します。
- **Use Shared Tree for the Groups specified below** : **Multicast Groups** テーブルで指定したグループに共有ツリーを使用するには、このオプションを選択します。**Multicast Groups** テーブルで指定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す。
- **Multicast Groups** : 共有ツリーを使用するマルチキャスト グループを表示します。

テーブル エントリは、上から下の順で処理されます。特定のグループの拒否ルールをテーブルの一番上に、マルチキャスト グループの範囲の許可ルールを deny 文の下にそれぞれ配置すれば、マルチキャスト グループの範囲を含みながらその範囲内の特定グループを除外するエントリを作成できます。

エントリをダブルクリックすると、選択したエントリを対象とした **Multicast Group** ダイアログボックスが開きます。

- **Action** : マルチキャスト グループが含まれる場合は「Permit」を、マルチキャスト グループが除外される場合は「deny」を表示します。

- Multicast Group Address : マルチキャスト グループのアドレスを表示します。
- Netmask : マルチキャスト グループアドレスのネットワーク マスクを表示します。
- Insert Before : **Multicast Group** ダイアログボックスが開きます。テーブルで選択したエントリの前に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- Insert After : **Multicast Group** ダイアログボックスが開きます。テーブルで選択したエントリの後に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- Add : **Multicast Group** ダイアログボックスが開きます。テーブルの一番下に新しいマルチキャスト グループ エントリを追加するには、このボタンを使用します。
- Edit : **Multicast Group** ダイアログボックスが開きます。選択したマルチキャスト グループ エントリの情報を変更するには、このボタンを使用します。
- Delete : 選択したマルチキャスト グループ エントリをテーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

