CHAPTER 17

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 モードでだけサポートされます。ここでは、次の内容について説明します。

- 「Multicast」（P.17-1）：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.17-2）：セキュリティ アプライアンスで IGMP を設定します。
- 「Multicast Route」（P.17-8）：スタティック マルチキャスト ルートを定義します。
- 「MBoundary」（P.17-10）：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.17-12）：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.17-13）：セキュリティ アプライアンスで PIM を設定します。

Multicast

[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。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が存在するかどうか学習するために使用されます。ホストは、IGMP 報告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。

（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。

フィールド

[Enable Multicast Routing]：このチェックボックスをオンにすると、セキュリティ アプライアンスでの IP マルチキャスト ルーティングがイネーブルになります。IP マルチキャスト ルーティングをディセーブルにする場合は、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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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）
「IGMP」（P.17-2）
「Multicast Route」（P.17-8）
「MBoundary」（P.17-10）
「MForwarding」（P.17-12）
「PIM」（P.17-13）

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 では、グループ アドレス（クラス D IP アドレス）が使用されます。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。

セキュリティ アプライアンスでの IGMP の設定に関する詳細については、次の各項目を参照してください。

- アクセス グループ
- Join Group
- Protocol
- Static Group

アクセス グループ

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 グループを制御するためのものです。

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 グループが表示されます。

  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ためのアクセス グループ エントリはテーブルの上方に配置し、許可ルールに指定されたグループなど、一定のまとまりを持った複数のマルチキャスト グループを拒否するようなアクセス グループ エントリは下方に配置します。ただし、拒否ルールよりも許可ルールの方が優先的に適用されるため、許可ルールに指定されているグループは、拒否ルールが適用された場合でも許可されます。

テーブルのエントリをダブルクリックすると、選択したエントリに対応する [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が表示されます。
  - [Action]：アクセス ルールにおいて、該当するマルチキャスト グループ アドレスが許可されている場合は、[Permit] が表示されます。アクセス ルールにおいて、該当するマルチキャスト グループ アドレスが拒否されている場合は、[Deny] が表示されます。
  - [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 アドレスが表示されます。
  - [Netmask]：マルチキャスト グループ アドレスのネットワーク マスクが表示されます。

- [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場合は、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場合は、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。テーブルの最後尾に新しいアクセス グループ エントリを追加する場合は、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場合は、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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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場合、一部のフィールドが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 グループを編集しているときは、関連インターフェイスは変更できません。
  - [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場合は [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場合は、[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 マスクをいずれか 1 つ選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Join Group

セキュリティ アプライアンスがマルチキャスト グループのメンバになるように設定できます。[Join Group] ペインには、セキュリティ アプライアンスがメンバになっているマルチキャスト グループが表示されます。

（注）　特定のグループのマルチキャスト パケットを、そのグループに属するセキュリティ アプライアンスに取得されることなく、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 メンバーシップが表示されます。
  - [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が表示されます。
  - [Multicast Group Address]：インターフェイスが属するマルチキャスト グループのアドレスが表示されます。
- [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場合は、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場合は、このボタンを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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場合は、[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場合は、[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ときは、この値は変更できません。
- [Multicast Group Address]：このフィールドには、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 の値である必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Protocol

[Protocol] ペインには、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 パラメータが表示されます。

フィールド

- [Protocol]：各インターフェイスに設定された IGMP パラメータが表示されます。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が表示されます。
  - [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] が表示されます。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] が表示されます。
  - [Version]：インターフェイス上でイネーブルになっている IGMP のバージョンが表示されます。
  - [Query Interval]：指定したルータから IGMP ホストクエリー メッセージが送信される時間間隔が秒単位で表示されます。
  - [Query Timeout]：インターフェイスのクエリアが停止してから、セキュリティ アプライアンスによりクエリアが引き継がれるまでの時間間隔が秒単位で表示されます。
  - [Response Time]：IGMP クエリーでアドバタイズされる最大応答時間が秒単位で表示されます。この設定への変更内容は、IGMP バージョン 2 に対してだけ有効です。
  - [Group Limit]：インターフェイスで許可される最大グループ数が表示されます。
  - [Forward Interface]：選択したインターフェイスから転送され IGMP ホスト レポートの転送先となるインターフェイスの名前が表示されます。
- [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

次の表は、この機能を使用できるモードを示したものです。

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

- [Name]：設定対象となるインターフェイスの名前が表示されます。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]：このチェックボックスをオンにすると、インターフェイスがイネーブルになります。インターフェイスで IGMP をディセーブルにする場合は、このチェックボックスをオフにします。セキュリティ アプライアンスでのマルチキャスト ルーティングをイネーブルにしてある場合、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。一部の機能では、IGMP バージョン 2 が必要になります。デフォルトの場合、セキュリティ アプライアンスで使用されるのは IGMP バージョン 2 です。
- [Query Interval]：指定したルータから IGMP ホストクエリー メッセージが送信される時間間隔を秒単位で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。
- [Query Timeout]：インターフェイスのクエリアが停止してから、セキュリティ アプライアンスによりクエリアが引き継がれるまでの時間間隔を秒単位で入力します。有効な値の範囲は 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単位で入力します。セキュリティ アプライアンスでは、指定した応答時間内にホスト レポートが受信できない場合、IGMP グループがプルーニングされます。この値を小さくすると、セキュリティ アプライアンスでグループのプルーニングが行われるまでの時間が短くなります。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加入する最大ホスト数を入力します。有効な値の範囲は 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場合、[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

次の表は、この機能を使用できるモードを示したものです。

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

Static Group

ネットワーク上のホストによっては、IGMP クエリーに応答しないよう設定されていることがあります。しかし、そうしたネットワーク セグメントに対しても、マルチキャスト トラフィックを転送することが必要となる場合もあります。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] ペインで、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。この方法を使用すると、セキュリティ アプライアンスでは、指定したインターフェイスにマルチキャスト パケットが転送されるだけでなく、そのパケットが取得されます。
- [Static Group] ペインで、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 メンバーとして設定します。この方法を使用した場合、セキュリティ アプライアンスでは、パケットが転送されるだけで、パケット自体は取得されません。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。

フィールド

- [Static Group] : 各インターフェイスに対してスタティックに割り当てられたマルチキャスト グループが表示されます。
  - [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が表示されます。
  - [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が表示されます。
- [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 グループを割り当てる場合は、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場合は、このボタンを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Add/Edit IGMP Static Group

インターフェイスに対してマルチキャスト グループをスタティックに割り当てる場合は、[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場合は、[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ときは、この値は変更できません。
- [Multicast Group Address]：このフィールドには、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 の値である必要があります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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、送信元と宛先の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は、その解決策として、2 つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

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、そのエントリに対応する [Add/Edit Multicast Route] ダイアログボックスが開きます。
  - [Source Address]：マルチキャスト送信元の IP アドレスとマスクが CIDR 表記で表示されます。
  - [Source Interface]：マルチキャスト ルートの着信インターフェイスが表示されます。
  - [Destination Interface]：マルチキャスト ルートの発信インターフェイスが表示されます。
  - [Admin Distance]：スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスが表示されます。
- [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 ルートを追加する場合は、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 ルートを変更する場合は、このボタンを使用します。
- [Delete]：選択したスタティック ルートを削除する場合は、このボタンを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Add/Edit Multicast Route

セキュリティ アプライアンスに新しいスタティック マルチキャスト ルートを追加する場合は、[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 ルートを変更する場合は、[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] : マルチキャスト送信元の 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、この値は変更できません。
- [Source Mask] : マルチキャスト送信元の 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、この値は変更できません。
- [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] :（任意）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、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 マルチキャスト ルートのアドミニストレーティブ ディスタンスがユニキャスト ルートのアドミニストレーティブ ディスタンスと同じである場合は、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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、その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、次の情報が表示されます。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が一覧表示されます。
- [Boundary Filter]：指定したインターフェイスの境界フィルタ エントリが一覧表示されます。このカラムでは、マルチキャスト境界が定義されていないインターフェイスに対して、「No Boundary Filters Configured」と表示されます。
- [AutoFilter]：Auto-RP メッセージが境界 ACL により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、Auto-RP メッセージのフローも ACL によって制限されます。[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。デフォルトでは、この機能はディセーブルになっています。

[Boundary] テーブルのエントリに対しては、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

次の表は、この機能を使用できるモードを示したものです。

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

Edit Boundary Filter

[Edit Boundary Filter] ダイアログボックスには、マルチキャスト境界フィルタ ACL が表示されます。このダイアログボックスを使用すれば、境界フィルタ ACL エントリを追加したり削除したりできます。

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、実行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。ただし、*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。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。

フィールド

- [Interface]：マルチキャスト境界フィルタ ACL を設定しているインターフェイスが表示されます。
- [Remove any Auto-RP group range]：境界 ACL により拒否された送信元からの Auto-RP メッセージをフィルタリングする場合は、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すると、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、次の情報が表示されます。

- [Action]：フィルタ エントリのアクションが表示されます。[Permit] が表示されている場合は、指定したトラフィックの通過が許可されます。[Deny] が表示されている場合は、指定したトラフィックによるインターフェイスの通過が拒否されます。インターフェイスに対してマルチキャスト境界フィルタが設定されている場合、デフォルトでは、マルチキャスト トラフィックは拒否されます。
- [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 アドレスが表示されます。
- [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 マスクが表示されます。

[Boundary Filter] テーブルに対しては、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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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が拒否されます。インターフェイスに対してマルチキャスト境界を設定すると、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 トラフィックが、インターフェイスの通過を拒否されます。
- [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

次の表は、この機能を使用できるモードを示したものです。

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

マルチキャスト転送がディセーブルになっているインターフェイスでは、他の方法で特に設定されていない限り、マルチキャスト パケットは取得されません。また、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、IGMP パケットも拒否されます。

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済みのインターフェイスが表示されます。インターフェイスを選択する場合は、その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] が表示されます。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] が表示されます。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について、[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

次の表は、この機能を使用できるモードを示したものです。

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

ルータでは、マルチキャスト データグラムの転送に使用する転送テーブルが、PIM を使用して管理されます。

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、すべてのインターフェイスでは PIM がデフォルトで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 の設定に関する詳細については、次の各項目を参照してください。

- Protocol
- 「Neighbor Filter」（P.17-14）
- 「Bidirectional Neighbor Filter」（P.17-16）
- Rendezvous Points
- Route Tree
- Request Filter

Protocol

[Protocol] ペインには、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、そのエントリに対応する [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が表示されます。
  - [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] が、イネーブルになっていない場合は [No] がそれぞれ表示されます。
  - [DR Priority]：インターフェイスの優先度が表示されます。
  - [Hello Interval]：インターフェイスから PIM hello メッセージが送信される時間間隔が、秒単位で表示されます。
  - [Join-Prune Interval]：インターフェイスから PIM の加入アドバタイズメントおよびプルーニング アドバタイズメントが送信される時間間隔が、秒単位で表示されます。
- [Edit]：選択したエントリに対応する [Edit PIM Protocol] ダイアログボックスが開きます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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]：*表示専用*。選択したインターフェイスの名前が表示されます。この値は編集できません。
- [PIM Enabled]：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 をイネーブルにできます。選択したインターフェイスで PIM をディセーブルにする場合は、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に対して指定ルータ優先度を設定します。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 0 に設定した場合は、そのセキュリティ アプライアンス インターフェイスがデフォルトのルータになることはありません。
- [Hello Interval]：インターフェイスから PIM hello メッセージが送信される時間間隔を秒単位で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 30 秒です。
- [Join-Prune Interval]：インターフェイスから PIM の加入アドバタイズメントおよびプルーニング アドバタイズメントが送信される時間間隔を秒単位で入力します。有効な値の範囲は、10 ～ 600 秒です。デフォルト値は 60 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Neighbor Filter

セキュリティ アプライアンスで設定された PIM ネイバー フィルタがもしあれば、[Neighbor Filter] ペインには、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、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、実行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。ただし *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。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスがセキュリティ アプライアンスの PIM ネイバーになれるか定義されます。

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、選択したエントリに対応する [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が表示されます。
- [Action]：指定したネイバーが PIM への参加を許可される場合は、[Permit] が表示されます。指定したネイバーが PIM への参加を拒否される場合は、[Deny] が表示されます。
- [Network Address]：許可または拒否されるネイバーのネットワーク アドレスが表示されます。
- [Netmask]：[Network Address] に表示されるアドレスとともに使用するネットワーク マスクが表示されます。

次の操作を実行できます。

- [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

次の表は、この機能を使用できるモードを示したものです。

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

詳細情報

「Add/Edit/Insert Neighbor Filter Entry」（P.17-15）

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 へ参加を許可されます。[Deny] を選択すると、指定したネイバーは PIM への参加を拒否されます。
- [Network Address]：許可または拒否されるネイバーのネットワーク アドレスが表示されます。
- [Netmask]：[Network Address] に表示されるアドレスとともに使用するネットワーク マスクが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Bidirectional Neighbor Filter

セキュリティ アプライアンスに PIM 双方向ネイバー フィルタが設定されている場合、[Bidirectional Neighbor Filter] ペインにそれらの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。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ければ、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。ただし *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。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスがセキュリティ アプライアンスの PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタでは、すべてのルータがスパース モード ドメインに参加できるようにしたまま、DF 選定に参加するルータを指定できるので、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への移行が可能になります。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタがイネーブルになると、ACL により許可され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。

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ます。エントリをダブルクリックして、そのエントリの [Edit Bidirectional Neighbor Filter Entry] ダイアログボックスを開きます。

- [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が表示されます。
- [Action]：双方向ネイバー フィルタにより DF 選定プロセスへの参加が許可される場合は、[Permit] が表示されます。そのエントリで、指定したアドレスが DF 選定プロセスへの参加を拒否される場合は、[Deny] が表示されます。
- [Network Address]：許可または拒否されているアドレスが表示されます。
- [Netmask]：[Network Address] に適用されるネットワーク マスクが表示されます。

次の操作を実行できます。

- [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

次の表は、この機能を使用できるモードを示したものです。

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

詳細情報

「Add/Edit/Insert Bidirectional Neighbor Filter Entry」（P.17-17）

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 選定への参加を許可される場合は、[Permit] を選択します。指定したデバイスが DF 選定への参加を拒否される場合は、[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 アドレスが表示されます。
- [Netmask]：[Network Address] に表示されるアドレスとともに使用するネットワーク マスクが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

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

Rendezvous Points

PIM を設定する場合は、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、共有配布ツリーの唯一かつ共通のルートで、各ルータでは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。

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。

フィールド

- [Generate IOS compatible register messages]：RP が Cisco IOS ルータの場合は、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 ソフトウェアでは、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ともに登録メッセージを受け取る方法）によってではなく、PIM ヘッダーにあるチェックサムとそれに続く 4 バイトと共に登録メッセージを受け取ります。
- [Rendezvous Points]：セキュリティ アプライアンスで設定された RP が表示されます。
  - [Rendezvous Point]：RP の IP アドレスが表示されます。
  - [Multicast Groups]：RP に関連付けられたマルチキャスト グループが表示されます。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--] が表示されます。
  - [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] が表示されます。指定したグループがスパース モードで動作する場合は、[No] が表示されます。
- [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場合は、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場合は、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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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、新しいエントリを [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 アドレスは、2 度使用できません。

- 複数の RP に対しては、[All Groups] を指定できません。

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 エントリを編集しているときは、この値は変更できません。
- [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、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、マルチキャスト パケットを受信したセキュリティ アプライアンスから送信元にプルーニング メッセージが戻されます。指定したマルチキャスト グループをスパース 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、実際の双方向コンフィギュレーションとは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

- [Use this RP for All Multicast Groups] : 指定した RP をインターフェイス上のすべてのマルチキャスト グループに対して使用する場合は、このオプションを選択します。
- [Use this RP for the Multicast Groups as specified below] : 指定した RP をマルチキャスト グループで使用するように指定する場合は、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 グループが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループを含みながら、その範囲の中から特定のグループが除外されるような RP エントリを作成する場合は、除外する特定のグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

  エントリをダブルクリックすると、選択したエントリに対応する [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] が、マルチキャスト グループが除外される場合は [Deny] がそれぞれ表示されます。
  - [Multicast Group Address] : マルチキャスト グループのアドレスが表示されます。
  - [Netmask] : マルチキャスト グループ アドレスのネットワーク マスクが表示されます。
- [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場合は、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ろに新しいマルチキャスト グループ エントリを追加する場合は、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。テーブルの最後尾に新しいマルチキャスト グループ エントリを追加する場合は、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場合は、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

次の表は、この機能を使用できるモードを示したものです。

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

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。1 つのマルチキャスト グループには、単独のマルチキャスト アドレスまたはある範囲に属する複数のマルチキャスト アドレス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 ルールを作成する場合は、[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 ルールを修正する場合は、[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 ルールを作成する場合は [Permit] を、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 ルールを作成する場合は [Deny] をそれぞれ選択します。
- [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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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場合、特定のマルチキャスト ソースをそれに登録できないように制限できます。これにより、未許可の送信元が RP に登録されることを回避できます。[Request Filter] ペインでは、セキュリティ アプライアンスで PIM 登録メッセージが受け入れられるマルチキャスト ソースを定義できます。

フィールド

- [Multicast Groups]：要求フィルタ アクセス ルールが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループを含みながら、その範囲の中から特定のグループが除外されるようなエントリを作成する場合は、除外する特定のグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

エントリをダブルクリックすると、選択したエントリに対応する [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] が、マルチキャストの送信元が除外される場合は [Deny] がそれぞれ表示されます。
  - [Source]：登録メッセージの送信元のアドレスが表示されます。
  - [Destination]：マルチキャストの宛先アドレスが表示されます。

- [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場合は、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ろに新しいマルチキャスト グループ エントリを追加する場合は、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。テーブルの最後尾に新しいマルチキャスト グループ エントリを追加する場合は、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場合は、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

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	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 として動作する場合に、セキュリティ アプライアンスに登録できるマルチキャスト送信元を定義できます。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 ルールを作成します。

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 アプライアンスへの登録を許可するルールを作成する場合は [Permit] を、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 アプライアンスへの登録を許可しないルールを作成する場合は [Deny] をそれぞれ選択します。
- [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		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

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。

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 ツリーを使用する場合は、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場合は、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場合は、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 グループが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループを含みながら、その範囲の中から特定のグループが除外されるようなエントリを作成する場合は、除外する特定のグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

  エントリをダブルクリックすると、選択したエントリに対応する [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] が、マルチキャスト グループが除外される場合は [Deny] がそれぞれ表示されます。
  - [Multicast Group Address] : マルチキャスト グループのアドレスが表示されます。
  - [Netmask] : マルチキャスト グループ アドレスのネットワーク マスクが表示されます。
- [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場合は、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ろに新しいマルチキャスト グループ エントリを追加する場合は、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。テーブルの最後尾に新しいマルチキャスト グループ エントリを追加する場合は、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場合は、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

次の表は、この機能を使用できるモードを示したものです。

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