マルチキャスト

この章では、マルチキャスト ルーティング プロトコルを使用するように Secure Firewall Threat Defense デバイス を設定する方法について説明します。

マルチキャスト ルーティングについて

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、送信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャスト プロトコルを使用した Firewall Threat Defense デバイス によりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

Firewall Threat Defense デバイス は、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つの Firewall Threat Defense デバイス に両方を同時に設定することはできません。

（注） マルチキャスト ルーティングでは、UDP トランスポートおよび非 UDP トランスポートの両方がサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

IGMP プロトコル

IP ホストは、Internet Group Management Protocol（IGMP）を使用して、そのグループ メンバーシップを、直接接続されているマルチキャスト ルータに報告します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP は、グループ アドレス（クラス D IP アドレス）をグループ識別子として使用します。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。

（注） Firewall Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、IGMP バージョン 2 がすべてのインターフェイスで自動的に有効になります。

マルチキャスト グループへのクエリ メッセージ

Firewall Threat Defense デバイスは、クエリ メッセージを送信して、インターフェイスに接続されているネットワークにメンバーを持つマルチキャスト グループを検出します。メンバーは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリ メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、Firewall Threat Defense デバイスに保存されているメンバーシップ情報が更新されます。Firewall Threat Defense デバイスで、ローカル メンバーがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャスト パケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上の PIM 代表ルータがクエリ メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリ応答時間を変更する場合は、IGMP クエリでアドバタイズする最大クエリ応答所要時間はデフォルトで 10 秒になります。Firewall Threat Defense デバイスがこの時間内にホスト クエリの応答を受信しなかった場合、グループを削除します。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、Firewall Threat Defense デバイス は IGMP のプロキシ エージェントとして動作します。Firewall

Threat Defense デバイス は、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、Firewall Threat Defense デバイス を PIM スパース モードまたは双方向モード用に設定できません。IGMP スタブ マルチキャスト ルーティングに参加するインターフェイス上で PIM を有効にする必要があります。

Firewall Threat Defense デバイス は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイント（RP）に転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルト ルートが RP に提供されます。

（注） Firewall Threat Defense デバイスが PIM RP の場合は、Firewall Threat Defense デバイスの変換されていない外部アドレスを RP アドレスとして使用してください。

PIM Source Specific Multicast のサポート

Firewall Threat Defense デバイスは PIM Source Specific Multicast（SSM）の機能や関連設定をサポートしていません。ただし、Firewall Threat Defense デバイスは最終ホップ ルータとして配置されていない限り、SSM 関連のパケットの通過を許可します。

SSM は、IPTV などの 1 対多のアプリケーションのデータ送信メカニズムとして分類されます。SSM モデルは、（S、G）ペアで示される「チャネル」の概念を使用します。S は発信元アドレス、G は SSM 宛先アドレスです。チャネルに登録するには、IGMPv3 などのグループ管理プロトコルを使用して行います。SSM は、特定のマルチキャスト送信元について学習した後、受信側のクライアントを有効にします。これにより、共有ランデブー ポイント（RP）からではなく、直接送信元からマルチキャスト ストリームを受信できるようになります。アクセス制御メカニズムは SSM 内に導入され、現在のスパースまたはスパース - デンス モードの実装では提供されないセキュリティ拡張機能を提供します。

PIM-SSM は、RP または共有ツリーを使用しない点で PIM-SM とは異なります。代わりに、マルチキャスト グループの発信元アドレスの情報は、ローカル受信プロトコル（IGMPv3）経由で受信者から提供され、送信元固有のツリーを直接作成するために使用されます。

マルチキャスト双方向 PIM

マルチキャスト双方向 PIM は、ビデオ会議、Webex ミーティング、およびグループチャットなどのように、同時に通信を行う送信元と受信者が多く存在し、各参加者がマルチキャスト トラフィックの送信元、受信者のどちらにもなりうるネットワークで有効です。PIM 双方向モードを使用すると、RP は共有ツリーの（*,G）エントリのみを作成します。（S,G）エントリはありません。各（S,G）エントリの状態テーブルを維持しないので、RP のリソースの節約になります。

PIM スパース モードでは、トラフィックは共有ツリーを下りにのみ流れます。PIM 双方向モードでは、トラフィックは共有ツリーの上りと下りの双方向に流れます。

PIM 双方向モードでは、PIM 登録/登録停止メカニズムを使って RP に送信元の登録をしません。送信元はそれぞれ、いつでもソースへの送信を開始できます。マルチキャスト パケットが RP に到達すると、共有ツリーで下りに転送されるか（受信者がいる場合）、ドロップされます（受信者がいない場合）。ただし、RP から送信元に対してマルチキャスト トラフィックの送信停止を命令する方法はありません。

設計の観点から、ネットワークのどこに RP を配置するかを考える必要があります。ネットワーク内の送信元と受信者の中間のどこかに配置する必要があるからです。

PIM 双方向モードには、リバース パス フォワーディング（RPF）のチェックがありません。ループを回避するため、代わりに代表フォワーダ（DF）の概念を使用します。この DF は、セグメント内で唯一、RP にマルチキャスト トラフィックの送信を許可されたルータです。マルチキャスト トラフィックを転送するルータがセグメントあたり 1 台だけであれば、ループは発生しません。DF は次のメカニズムを使って選択されます。

- RP へのメトリックが最も小さいルータが DF になる。
- メトリックが等しい場合は、IP アドレスが最も大きいルータが DF になる。

PIM ブートストラップ ルータ（BSR）

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 メッセージ経由で、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。

この機能は、RP を動的に学習する方法を提供するため、RP が停止と起動を繰り返す複雑で大規模なネットワークには不可欠です。

PIM ブートストラップ ルータ（BSR）の用語

PIM BSR の設定では、次の用語がよく使用されます。

- ブートストラップ ルータ（BSR）：BSR はホップバイホップ ベースの PIM が設定された他のルータに、ランデブー ポイント（RP）情報をアドバタイズします。選択プロセスの後に、複数の候補 BSR の中から 1 つの BSR が選択されます。このブートストラップ ルータの主な目的は、すべての候補 RP（C-RP）通知を RP-set というデータベースに収集し、これをネットワーク内の他のすべてのルータに定期的に BSR メッセージとして送信することです（60 秒ごと）。
- ブートストラップ ルータ（BSR）メッセージ：BSR メッセージは、TTL が 1 に設定された All-PIM-Routers グループへのマルチキャストです。これらのメッセージを受信するすべての PIM ネイバーは、メッセージを受信したインターフェイスを除くすべてのインターフェイスからそのメッセージを再送信します（TTL は 1 に設定）。BSR メッセージには、現在アクティブな BSR の RP-set と IP アドレスが含まれています。この方法で、C-RP は C-RP メッセージのユニキャスト先を認識します。
- 候補ブートストラップ ルータ（C-BSR）：候補 BSR として設定されるデバイスは、BSR 選択メカニズムに参加します。最も優先順位の高い C-BSR が BSR として選択されます。C-BSR の最上位の IP アドレスはタイブレイカーとして使用されます。BSR の選択プロセスはプリエンプティブです。たとえば、より優先順位の高い C-BSR が新たに見つかると、新しい選択プロセスがトリガーされます。
- 候補ランデブーポイント（C-RP）：RP はマルチキャストデータの送信元と受信者が対面する場所として機能します。C-RP として設定されているデバイスは、マルチキャスト グループ マッピング情報を、ユニキャスト経由で直接、選択された BSR に定期的にアドバタイズします。これらのメッセージには、グループ範囲、C-RP アドレス、および保留時間が含まれています。現在の BSR の IP アドレスは、ネットワーク内のすべてのルータが受信した定期的な BSR メッセージから学習されます。このようにして、BSR は現在動作中で到達可能な RP 候補について学習します。

（注） C-RP は BSR トラフィックの必須要件ですが、Firewall Threat Defense デバイス は C-RP としては機能しません。ルータのみが C-RP として機能できます。したがって、BSR のテスト機能では、トポロジにルータを追加する必要があります。

- BSR 選択メカニズム：各 C-BSR は、BSR 優先順位フィールドを含むブートストラップ メッセージ（BSM）を生成します。ドメイン内のルータは、ドメイン全体に BSM をフラッディングします。自身より優先順位の高い C-BSR に関する情報を受け取った BSR は、一定期間、BSM の送信を抑止します。残った単一の C-BSR が選択された BSR となり、その BSM により、選択された BSR に関する通知がドメイン内の他のすべてのルータに対して送信されます。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界

がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMPを使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。

マルチキャスト アドレス

マルチキャストアドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタ

マルチキャスト ルーティングは、クラスタリングをサポートします。スパンドEtherChannelクラスタリングでは、ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを送信します。ファーストパス転送が確立されると、データユニットがマルチキャストデータ パケットを転送できます。すべてのデータ フローは、フル フローです。スタブ転送フローもサポートされます。スパンドEtherChannelクラスタリングでは 1 つのユニットだけがマルチキャストパケットを受信するため、制御ユニットへのリダイレクションは共通です。

マルチキャストルーティングの要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

マルチキャスト ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6

IPv6 はサポートされません。

マルチキャスト グループ

224.0.0.0 ー 224.0.0.255 のアドレス範囲は、ルーティングプロトコル、およびゲートウェイディスカバリやグループ メンバーシップ レポートなどのその他のトポロジディスカバリまたはメンテナンスプロトコルを使用するために予約されています。したがって、アドレス範囲224.0.0/24からのインターネット マルチキャスト ルーティングはサポートされません。予約されたアドレスのマルチキャストルーティングを有効にすると、IGMP グループは作成されません。

クラスタリング

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

- 224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンド セキュリティ ゾーン上のアクセス制御またはプレフィルタ ルールを設定する必要があります。ただし、ルールの宛先セキュリティゾーンを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。
- PIM が設定されているインターフェイスは無効にできません。インターフェイスで PIM を設定している場合（PIMプロトコルの設定（14ページ）を参照）、マルチキャストルーティングと PIM を無効にしても PIM 設定は削除されません。インターフェイスを無効にするには、PIM 設定を削除する必要があります。
- PIM/IGMP マルチキャストルーティングは、トラフィックゾーン内のインターフェイスではサポートされません。
- Firewall Threat Defense を同時にランデブーポイント（RP）とファーストホップルータになるように設定しないでください。
- HSRP スタンバイ IP アドレスは、PIM ネイバーシップに参加しません。したがって、RP ルータ IP が HSRP スタンバイ IP アドレスを介してルーティングされる場合、マルチキャストルーティングはFirewall Threat Defenseで機能しません。マルチキャストトラフィックが正常に通過するようにするには、RP アドレスのルートが HSRP スタンバイ IP アドレスではないことを確認し、代わりに、ルートアドレスをインターフェイス IP アドレスに設定します。
- 仮想ルーティングを使用しているデバイスの場合、ユーザ定義の仮想ルータではなく、グローバル仮想ルータに対してのみマルチキャストを設定できます。

IGMP 機能の設定

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、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

手順

ステップ 1 マルチキャスト ルーティングの有効化 （8 ページ）。
ステップ 2 IGMP プロトコルの設定 （9 ページ）。
ステップ 3 IGMP アクセスグループの設定 （11 ページ）。
ステップ 4 IGMP スタティック グループの設定 （12 ページ）。
ステップ 5 IGMP 参加グループの設定 （13 ページ）。

マルチキャスト ルーティングの有効化

Firewall Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、デフォルトですべてのインターフェイス上の IGMP と PIM が有効になります。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ー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 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。

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

以下の一覧に、特定のマルチキャストテーブルに追加されるエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

- MFIB：30,000
- IGMP グループ：30,000
- PIM ルート：72,000

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 Choose **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [マルチキャスト ルーティングの有効化（Enable Multicast Routing）] チェックボックスをオンにします。

このチェックボックスをオンにすると、デバイス上で IP マルチキャストルーティングが有効になります。このチェックボックスをオフにすると、IP マルチキャスト ルーティングが無効になります。デフォルトでは、マルチキャストは無効になっています。マルチキャスト ルーティングを有効にすると、すべてのインターフェイス上でマルチキャストが有効になります。

マルチキャストはインターフェイスごとに無効にできます。この情報が役に立つのは、あるインターフェイス上にマルチキャスト ホストがないことがわかっている場合に、そのインターフェイス上で Firewall Threat Defense デバイスからホスト クエリ メッセージが送信されないように設定するときです。

IGMP プロトコルの設定

転送インターフェイス、クエリ メッセージ、時間間隔などのインターフェイスごとに、IGMP パラメータを設定できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [Protocol] で、[Add] または [Edit] をクリックします。

[IGMP パラメータの追加（Add IGMP parameters）] ダイアログボックスで、Firewall Threat Defense デバイスに新しい IGMP パラメータを追加します。既存のパラメータを変更する場合は、[IGMP パラメータの編集（Edit IGMP parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウンリストから、IGMP プロトコルを設定するインターフェイスを選択します。

- [IGMP を有効にする（Enable IGMP）]：IGMP を有効にするには、このチェックボックスをオンにします。

  （注）
  特定のインターフェイスでIGMPを無効にすることは、あるインターフェイス上にマルチキャストホストがないことがわかっている場合に、そのインターフェイス上でデバイスがホストクエリーメッセージを送信しないように設定するときに役に立ちます。

- [インターフェイスの転送（Forward Interface）]：ドロップダウンリストから、どのインターフェイスから IGMP メッセージを送信するかを選択します。

  これは Secure Firewall Threat Defense デバイスを、IGMP プロキシ エージェントとして設定し、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送します。

- [バージョン（Version）]：IGMP バージョン 1 または 2 を選択します。

  デフォルトでは、Firewall Threat Defense デバイスで IGMP バージョン 2 が実行されるため、多数の追加機能が使用できるようになります。

  （注）
  サブネットのマルチキャストルータはすべて、同じIGMPバージョンをサポートしている必要があります。Firewall Threat Defense デバイスが自動的にバージョン 1 ルータを検出してバージョン 1 に切り替えることはありません。ただ、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストを混在させることも可能です。IGMP バージョン 2 を実行している Firewall Threat Defense デバイスは、IGMP バージョン 1 のホストが存在しても正常に動作します。

- [クエリー インターバル（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秒単位の時間間隔。指定できる範囲は 1 ～ 3600 です。デフォルトは 125 です。

  （注）
  指定されたタイムアウト値の時間が経過しても、Firewall Threat Defense デバイスがインターフェイス上でクエリーメッセージを検出できなかった場合は、そのデバイスが指定ルータになり、クエリーメッセージの送信を開始します。

- [応答時間（Response Time）]：Firewall Threat Defense デバイスでグループが削除される前の秒単位の時間間隔。指定できる範囲は 1 ～ 25 です。デフォルトは 10 です。

  Firewall Threat Defenseデバイスがこの時間内にホストクエリーの応答を受信しなかった場合、グループを削除します。

- [グループ制限（Group Limit）]：インターフェイス上で加入する最大ホスト数。指定できる範囲は 1 ～ 500 です。デフォルトは 500 です。

  IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告はIGMPキャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

- [クエリータイムアウト（Query Timeout）]：秒単位の時間で、前のリクエスタがリクエスタとしての動作を停止してからこの時間が経過すると、この Firewall Threat Defense デバイスがそのインターフェイスのリクエスタの役割を引き継ぎます。指定できる範囲は 60 ～ 300 です。デフォルトは 255 です。

ステップ 5 [OK] をクリックして、IGMP プロトコル構成を保存します。

IGMP アクセスグループの設定

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）]>[マルチキャストルーティング（Multicast Routing）]>[アクセスグループ（Access Group）] を選択します。 > >

ステップ 3 [アクセスグループ（Access Group）] で、[追加（Add）] または [編集（Edit）] をクリックします。

[IGMP アクセス グループ パラメータを追加（Add IGMP Access Group parameters）] ダイアログボックスを使用して、新しい IGMP アクセスグループをアクセスグループ テーブルに追加します。既存のパラメータを変更する場合は、[IGMP アクセス グループ パラメータを編集（Edit IGMP Access Group parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

a) [インターフェイス（Interface）] ドロップダウンリストから、アクセスグループが関連付けられる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。

b) 次のいずれかをクリックします。

- [標準アクセスリスト（Standard Access List）]：[標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋) をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定を参照してください。
- [拡張アクセスリスト（Extended Access List）]：[拡張アクセスリスト（Extended Access List）] ドロップダウンリストから、拡張 ACL を選択するか、または [追加（Add）] (＋) をクリックして新しい拡張 ACL を作成します。手順については、拡張 ACL オブジェクトの設定を参照してください。

ステップ 5 [OK] をクリックして、アクセスグループ構成を保存します。

IGMP スタティック グループの設定

グループ メンバーがグループのメンバーシップをレポートできなかったり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信しなければならないことがあります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。この方法の場合、Firewall Threat Defense デバイスはパケットそのものを受信せず、転送だけを実行します。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 キャッシュ内に存在しますが、このインターフェイスはマルチキャスト グループのメンバーではありません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [スタティックグループ（Static Group）] で、[追加（Add）] または [編集（Edit）] をクリックします。

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、[IGMP スタティック グループ パラメータの追加（Add IGMP Static Group parameters）] 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、[IGMP スタティック グループ パラメータの編集（Edit IGMP Static Group parameters）] ダイアログボックスを使用します。

（注）
IGMP 静的グループを使用すると、PIM は送信元またはランデブーポイント（RP）向けに参加要求を送信できます。ただし、このコマンドのファイアウォールは、コマンドが適用されるインターフェイス上の PIM 代表ルータ（DR）であることが条件です。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、マルチキャストグループを静的に割り当てるインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [マルチキャストグループ（Multicast Groups）] ドロップダウンリストから、インターフェイスを割り当てるマルチキャストグループを選択するか、[追加（Add）] (＋) をクリックして新しいマルチキャストグループを作成します。手順については、Creating Network Objects を参照してください。

ステップ 5 [OK] をクリックして、スタティック グループ設定を保存します。

IGMP 参加グループの設定

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できます。マルチキャストグループに加入するように Firewall Threat Defense デバイスを設定すると、アップストリームルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注） IGMP スタティック グループの設定 （12 ページ）を参照して、特定のグループのマルチキャストパケットを特定のインターフェイスに転送する必要がある場合に、Firewall Threat Defense デバイスがそのパケットをそのグループの一部として受け付けることがないようにする方法を確認してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [IGMP] を選択します。 > >

ステップ 3 [参加グループ（Join Group）] で、[追加（Add）] または [編集（Edit）] をクリックします。

Firewall Threat Defense デバ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、[IGMP 参加グループ パラメータの追加（Add IGMP Join Group parameters）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[IGMP 参加グループ パラメータの編集（Edit IGMP Join Group parameters）] ダイアログボックスを使用します。

（注）
IGMP 参加グループを使用すると、PIM は送信元またはランデブーポイント（RP）向けに参加要求を送信できます。ただし、このコマンドのファイアウォールは、コマンドが適用されるインターフェイス上の PIM 代表ルータ（DR）であることが条件です。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、マルチキャストグループのメンバーにするインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [参加グループ（Join Group）] ドロップダウンリストから、インターフェイスを割り当てるマルチキャストグループを選択するか、[プラス（Plus）] をクリックして、新しいマル

チキャストグループを作成します。手順については、Creating Network Objects を参照してください。

PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。Secure Firewall Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、PIM および IGMP がすべてのインターフェイスで自動的に有効になります。

（注） PIM は、PAT ではサポートされません。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に対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

手順

ステップ 1 PIM プロトコルの設定 （14 ページ）。
ステップ 2 PIM ネイバー フィルタの設定 （15 ページ）。
ステップ 3 PIM 双方向ネイバー フィルタの設定 （16 ページ）。
ステップ 4 PIM ランデブー ポイントの設定 （18 ページ）。
ステップ 5 PIM ルート ツリーの設定 （19 ページ）。
ステップ 6 PIM リクエスト フィルタの設定 （20 ページ）。
ステップ 7 マルチキャスト境界フィルタの設定 （23 ページ）。

PIM プロトコルの設定

PIM は、特定のインターフェイスで有効または無効にすることができます。

代表ルータ（DR）のプライオリティを設定することもできます。DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。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、Firewall Threat Defense デバイスの DR プライオリティは 1 です。

ルータ クエリ メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリ メッセージを送信します。デフォルトでは、ルータ クエリ メッセージは 30 秒間隔で送信されま

す。さらに、60秒ごとに、Firewall Threat Defenseデバイスは PIM 加入メッセージおよびプルーニング メッセージを送信します。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [Protocol] で、[Add] または [Edit] をクリックします。

インターフェイスに新しい PIM パラメータを追加する場合は、[PIM パラメータの追加（Add PIM parameters）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM パラメータの編集（Edit PIM parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストから、PIM プロトコルを設定するインターフェイスを選択します。
- [PIM を有効にする（Enable PIM）]：PIM を有効にするには、このチェックボックスをオンにします。
- [DR プライオリティ（DR Priority）]：選択したインターフェイスの DR の値。サブネット上のルータのうち、DR プライオリティが最も大きいもの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 Firewall Threat Defense デバイスインターフェイスが指定ルータになることはありません。
- [Hello 間隔（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（秒単位）。指定できる範囲は 1 ～ 3600 です。デフォルトは 30 です。
- [参加プルーニング間隔（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（秒単位）。指定できる範囲は 10 ～ 600 です。デフォルトは 60 です。

ステップ 5 [OK] をクリックして、PIM プロトコル設定を保存します。

PIM ネイバー フィルタの設定

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャストルーティング（Multicast Routing）]** > **[PIM]** を選択します。

ステップ 3 [ネイバーフィルタ（Neighbor Filter）] で、[追加（Add）] または [編集（Edit）] をクリックします。

インターフェイスに新しい PIM ネイバー フィルタを追加する場合は、[PIM ネイバー フィルタの追加（Add PIM Neighbor Filter）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM ネイバー フィルタの編集（Edit PIM Neighbor Filter）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、PIM ネイバーフィルタを追加するインターフェイスを選択します。
- [標準アクセスリスト（Standard Access List）]：[標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋) をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定を参照してください。

（注）
[標準アクセス リスト エントリの追加（Add Standard Access List Entry）] ダイアログボックスで [許可（Allow）] を選択すると、マルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できるようになります。[ブロック（Block）] 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はこのインターフェイスを通過できなくなります。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。

ステップ 5 [OK] をクリックして、PIM ネイバー フィルタ設定を保存します。

PIM 双方向ネイバー フィルタの設定

PIM 双方向ネイバー フィルタは、Designated Forwarder（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。

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。DF を選択するために、セグメント内のすべてのマルチキャスト ルータが双方向で有効になっている必要があります。

PIM 双方向ネイバー フィルタが有効な場合、その ACL によって許可されるルータは、双方向に対応しているとみなされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向モードをサポートしていない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしている場合、DF選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしていない場合、DF 選択が実行される可能性があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [マルチキャスト ルーティング（Multicast Routing）] > [PIM] を選択します。

ステップ 3 [双方向ネイバーフィルタ（Bidirectional Neighbor Filter）] で、[追加（Add）] または [編集（Edit）] をクリックします。

PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成する場合は、[PIM 双方向ネイバーフィルタの追加（Add PIM Bidirectional Neighbor Filter）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM 双方向ネイバー フィルタの編集（Edit PIM Bidirectional Neighbor Filter）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウン リストから、PIM 双方向ネイバー フィルタの ACL エントリを設定するインターフェイスを選択します。
- [標準アクセスリスト（Standard Access List）] : [標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋)をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定を参照してください。

  （注）
  [標準アクセス リスト エントリの追加（Add Standard Access List Entry）] ダイアログボックスで [許可（Allow）] を選択すると、指定したデバイスが DR 選択プロセスに参加できます。[ブロック（Block）] を選択すると、指定したデバイスは DR 選択プロセスに参加できなくなります。

ステップ 5 [OK] をクリックして、PIM 双方向ネイバー フィルタ設定を保存します。

PIM ランデブー ポイントの設定

Firewall Threat Defense デバイスを複数のグループの RP として機能するように設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、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。双方向 PIM の詳細については、マルチキャスト双方向 PIM（4 ページ）を参照してください。

RP には、次の制約事項が適用されます。

- 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、[すべてのグループ（All Groups）] を指定できません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ランデブーポイント（Rendezvous Points）] で、[追加（Add）] または [編集（Edit）] をクリックします。

[ランデブーポイント（Rendezvous Points）]テーブルに新しいエントリを作成する場合は、[ランデブー ポイントの追加（Add Rendezvous Point）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[ランデブー ポイントの編集（Edit Rendezvous Point）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [ランデブーポイントのIPアドレス（Rendezvous Point IP address）] ドロップダウンリストから、RP として追加する IP アドレスを選択するか、[追加（Add）] (+) をクリックして新しいネットワークオブジェクトを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。
- [双方向転送の使用（Use bi-directional forwarding）] チェックボックスをオンにすると、指定されているマルチキャスト グループは双方向モードで動作します。双方向モードでは、Firewall Threat Defense デバイスがマルチキャスト パケットを受信したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にプルーニング メッセージが返されます。
- 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、[すべてのマルチキャストグループに対してこのRPを使用する（Use this RP for All Multicast Groups）] をクリックします。
- [次に指定するようにすべてのマルチキャストグループに対してこのRPを使用する（Use this RP for all Multicast Groups as specified below）] をクリックして、指定の RP とともに使

用するマルチキャストグループを指定します。次に [標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）] (＋) をクリックして、新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定を参照してください。

ステップ 5 [OK] をクリックして、ランデブー ポイント設定を保存します。

PIM ルート ツリーの設定

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。この方法では、遅延が短縮されますが、共有ツリーに比べて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、Firewall Threat Defense デバイスを最短パス ツリーに加入させるか、共有ツリーを使用するかを設定できます。

[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] テーブルには、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 グループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外する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。

（注） この動作は Shortest Path Switchover（SPT）と呼ばれます。[共有ツリー（Shared Tree）] オプションを常に使用することをお勧めします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ルートツリー（Route Tree）] で、ルートツリーのパスを選択します。

- 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、[最短パス（Shortest Path）] をクリックします。
- 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、[共有ツリー（Shared Tree）] をクリックします。
- [次に示すグループの共有ツリー（Shared tree for below mentioned group）] をクリックして、[マルチキャストグループ（Multicast Groups）] テーブルで指定されたグループを指定しま

す。次に [標準アクセスリスト（Standard Access List）] ドロップダウンリストから標準 ACL を選択するか、[追加（Add）](+)をクリックして、新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定を参照してください。

ステップ 4 [OK] をクリックして、ルート ツリー設定を保存します。

PIM リクエスト フィルタの設定

Firewall Threat Defense デバイスが RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。Firewall Threat Defense デバイスが PIM 登録メッセージを受け入れるマルチキャスト送信元を定義できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャストルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [リクエストフィルタ（Request Filter）] で、RP として動作する Firewall Threat Defense デバイスに登録できるマルチキャスト送信元を定義します。

- [PIM 登録メッセージのフィルタ方法：（Filter PIM register messages using:）] ドロップダウン リストから [なし（None）]、[アクセス リスト（Access List）]、または [ルート マップ（Route Map）] を選択します。
- ドロップダウンリストから [アクセスリスト（Access List）] を選択した場合は、拡張 ACL を選択するか、[追加（Add）](+) をクリックして新しい拡張 ACL を作成します。手順については、拡張 ACL オブジェクトの設定を参照してください。

  （注）
  [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、ドロップダウンリストから [許可（Allow）] を選択して、指定したマルチキャストトラフィックの指定した送信元を Firewall Threat Defense デバイスに登録することを許可するルールを作成します。または、[ブロック（Block）] を選択して、指定したマルチキャストトラフィックの指定した送信元がデバイスに登録されることを防ぐルールを作成します。

- [ルートマップ（Route Map）] を選択した場合は、[ルートマップ（Route Map）] ドロップダウンリストからルートマップを選択するか、[追加（Add）] (+) をクリックして新しいルートマップを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。

ステップ 4 [OK] をクリックして、リクエスト フィルタ設定を保存します。

Secure Firewall Threat Defense デバイスのブートストラップ ルータ設定

Firewall Threat Defense デバイスを BSR 候補として設定できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[PIM]** を選択します。

ステップ 3 [ブートストラップルータ（Bootstrap Router）] で、[このFTDをブートストラップルータ候補として設定（Configure this FTD as a Candidate Bootstrap Router (C-BSR)）] チェックボックスをオンにして、C-BSR の設定をします。

a) [インターフェイス（Interface）] ドロップダウンリストから、BSR アドレスが派生する Firewall Threat Defense デバイスのインターフェイスを選択して、候補にします。

このインターフェイスは PIM を使用して有効化する必要があります。

b) [ハッシュ マスク長（Hash mask length）] フィールドに、ハッシュ関数が呼び出される前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）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 RP に対応します。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。指定できる範囲は 0 ～ 32 です。

c) [優先度（Priority）] フィールドに、BSR 候補の優先度を入力します。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。指定できる範囲は 0 ～ 255 です。デフォルト値は 0 です。

ステップ 4 （オプション）[このFTDをボーダーブートストラップルータとして設定（Configure this FTD as a Border Bootstrap Router (BSR)）] セクションで、[追加（Add）] (+) をクリックして、PIM BSR メッセージを送受信しないインターフェイスを選択します。

- [インターフェイス（Interface）] ドロップダウンリストから、PIM BSR メッセージを送受信しないインターフェイスを選択します。

  RP または BSR アドバタイズメントは、フィルタリングされている効果的に隔てられた 2 つの RP 情報交換ドメインです。

- BSR を有効化するには、[ボーダー BSR を有効にする（Enable Border BSR）] チェックボックスをオンにします。

ステップ 5 [OK] をクリックして、ブートストラップ ルータ設定を保存します。

マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、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。

PIM を使用する場合、Firewall Threat Defense デバイスは、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで1つのパスを使用し、マルチキャスト パケットで別の1つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャストルーティング（Multicast Routing）]** > **[マルチキャストルート（Multicast Routes）]** > **[追加（Add）]** または **[編集（Edit）]** を選択します。

Firewall Threat Defense デバイスに新しいマルチキャスト ルートを追加する場合は、[マルチキャスト ルート設定の追加（Add Multicast Route Configuration）] 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 ルートを変更する場合は、[マルチキャスト ルート設定の編集（Edit Multicast Route Configuration）] ダイアログボックスを使用します。

ステップ 3 [送信元ネットワーク（Source Network）] ドロップダウンボックスから、既存のネットワークを選択するか、[追加（Add）] (+) をクリックして新しいネットワークを追加します。手順については、Creating Network Objects を参照してください。

ステップ 4 ルートを転送するようインターフェイスを設定するには、[インターフェイス（Interface）] をクリックして、以下のオプションを設定します。

- [送信元インターフェイス（Source Interface）] ドロップダウンリストから、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。
- [発信インターフェイス/デンス（Output Interface/Dense）] ドロップダウンリストから、ルートが転送される宛先インターフェイスを選択します。
- [距離（Distance）] フィールドに、マルチキャスト ルートの距離を入力します。指定できる範囲は 0 ～ 255 です。

ステップ 5 ルートを転送するよう RPF アドレスを設定するには、[アドレス（Address）] をクリックして、以下のオプションを設定します。

- [RPF アドレス（RPF Address）] フィールドに、マルチキャスト ルートの IP アドレスを入力します。
- [距離（Distance）] フィールドに、マルチキャスト ルートの距離を 0 ～ 255 で入力します。

ステップ 6 [OK] をクリックして、マルチキャスト ルータの設定を保存します。

マルチキャスト境界フィルタの設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界フィルタを定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界フィルタを設定できます。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープアドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であるとみなされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界フィルタが設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界フィルタを定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界での Auto-RP 検出および通知のメッセージの設定、検査、フィルタリングを行うことができます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界フィルタを通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [マルチキャスト境界フィルタ（Multicast Boundary Filter）]** を選択し、[追加（Add）] または [編集（Edit）] をクリックします。

[マルチキャスト境界フィルタの追加（Add Multicast Boundary Filter）] ダイアログボックスを使用して、新しいマルチキャスト境界フィルタをデバイスに追加します。既存のパラメータを変更するには、[マルチキャスト境界フィルタの編集（Edit Multicast Boundary Filter）] ダイアログボックスを使用します。

管理スコープ 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。

ステップ 3 [インターフェイス（Interface）] ドロップダウン リストから、マルチキャスト境界フィルタ ACL を設定するインターフェイスを選択します。

ステップ 4 [標準アクセスリスト（Standard Access List）] ドロップダウンリストから、使用する標準 ACL を選択するか、[追加（Add）](+)をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定を参照してください。

ステップ 5 境界 ACL によって拒否されたソースからの Auto-RP メッセージをフィルタするには、[境界によって拒否された Auto-RP パケットからの Auto-RP グループ範囲通知の削除（Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary）] チェックボックスをオンにします。このチェックボックスをオンにしていない場合、すべての Auto-RP メッセージが通過します。

ステップ 6 [OK] をクリックして、マルチキャスト境界フィルタの設定を保存します。

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。