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 device を設定する方法について説明します。

About Multicast Routing

Multicast routing is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast routing include videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Multicast routing protocols deliver source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by Firewall Threat Defense device enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols, which results in the most efficient delivery of data to multiple receivers possible.

The Firewall Threat Defense device supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single Firewall Threat Defense device.

（注） The UDP and non-UDP transports are both supported for multicast routing. However, the non-UDP transport has no FastPath optimization.

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。

Stub Multicast Routing

Stub multicast routing provides dynamic host registration and facilitates multicast routing. When configured for stub multicast routing, the Firewall Threat Defense device acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the Firewall Threat Defense device forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub

multicast routing, the Firewall Threat Defense device cannot be configured for PIM sparse or bidirectional mode. You must enable PIM on the interfaces participating in IGMP stub multicast routing.

The Firewall Threat Defense device supports both PIM-SM and bidirectional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a single Rendezvous Point (RP) per multicast group and optionally creates shortest-path trees per multicast source.

PIM Multicast Routing

Bidirectional PIM is a variant of PIM-SM that builds bidirectional shared trees connecting multicast sources and receivers. Bidirectional trees are built using a Designated Forwarder (DF) election process operating on each link of the multicast topology. With the assistance of the DF, multicast data is forwarded from sources to the Rendezvous Point (RP), and therefore along the shared tree to receivers, without requiring source-specific state. The DF election takes place during RP discovery and provides a default route to the RP.

（注） If the Firewall Threat Defense device is the PIM RP, use the untranslated outside address of the Firewall Threat Defense device as the RP address.

PIM Source Specific Multicast Support

Firewall Threat Defense device can forward source specific multicast traffic (e.g., for groups in the 232.x.x.x range) even though they do not support PIM-SSM configuration or Internet Group Management Protocol version 3 (IGMPv3).

SSM is classified as a data delivery mechanism for one-to-many applications such as IPTV. The SSM model uses a concept of "channels" denoted by an (S,G) pair, where S is a source address and G is an SSM destination address. Subscribing to a channel is achieved by using a group management protocol such as IGMPv3. SSM enables a receiving client, once it has learned about a particular multicast source, to receive multicast streams directly from the source rather than receiving it from a shared Rendezvous Point (RP). Access control mechanisms are introduced within SSM providing a security enhancement not available with current sparse or sparse-dense mode implementations.

Limitation:

- ASA cannot act as the last-hop router for SSM multicast because it does not support IGMPv3 (which receivers use to join SSM groups).

  If the ASA is the last-hop, it will ignore IGMPv3 join messages from receivers for SSM groups, and SSM forwarding will not work.

- Static multicast routes on ASA do not work for SSM range (232.x.x.x).

Workaround:

For Cisco ASA firewall to forward SSM-related multicast traffic, you must add a multicast-capable layer 3 device (such as a router or switch) that supports PIM and IGMPv3 on the same network segment as the receivers.

How it Works:

- Receivers register their SSM group joins (IGMPv3) with this layer 3 device.
- This layer 3 device sends PIM join messages towards the ASA.
- The ASA receives these PIM messages and dynamically learns multicast routes.
- SSM multicast traffic is then properly forwarded by the ASA, since it is no longer the last-hop device.

PIM-SSM differs from PIM-SM in that it does not use an RP or shared trees. Instead, information on source addresses for a multicast group is provided by the receivers through the local receivership protocol (IGMPv3) and is used to directly build source-specific trees.

Multicast Bidirectional PIM

Multicast bidirectional PIM is useful for networks that have many sources and receivers talking to each other simultaneously and where each participant can become both the source and receiver of multicast traffic, such as in videoconferencing, Webex meetings, and group chat. When PIM bidirectional mode is used, the RP only creates the (*,G) entry for the shared tree. There is no (S,G) entry. This conserves resources on the RP because state tables for each (S,G) entry are not maintained.

In PIM sparse mode, traffic only flows down the shared tree. In PIM bidirectional mode, traffic flows up and down the shared tree.

PIM bidirectional mode also does not use the PIM register/register-stop mechanism to register sources to the RP. Each source can begin sending to the source at any time. When the multicast packets arrive at the RP, they are forwarded down the shared tree (if there are receivers) or dropped (when there are no receivers). However, there is no way for the RP to tell the source to stop sending multicast traffic.

Design-wise you must think about where to place the RP in your network because it should be somewhere in the middle between the sources and receivers in the network.

PIM bidirectional mode has no Reverse Path Forwarding (RPF) check. Instead it uses the concept of a Designated Forwarder (DF) to prevent loops. This DF is the only router on the segment that is allowed to send multicast traffic to the RP. If there is only one router per segment that forwards multicast traffic, there will be no loops. The DF is chosen using the following mechanism:

- The router with the lowest metric to the RP is the DF.
- If the metric is equal, then the router with the highest IP address becomes the DF.

PIM Bootstrap Router (BSR)

PIM Bootstrap Router (BSR) is a dynamic Rendezvous Point (RP) selection model that uses candidate routers for RP function and for relaying the RP information for a group. The RP function includes RP discovery and provides a default route to the RP. It does this by configuring a set of devices as candidate BSRs (C-BSR) which participate in a BSR election process to choose a BSR amongst themselves. Once the BSR is chosen, devices that are configured as candidate Rendezvous Points (C-RP) start sending their group mapping to the elected BSR. The BSR then distributes the group-to-RP mapping information to all the other devices down the multicast tree through BSR messages that travel from PIM router to PIM router on a per-hop basis.

This feature provides a means of dynamically learning RPs, which is very essential in large complex networks where an RP can periodically go down and come up.

PIM Bootstrap Router (BSR) Terminology

The following terms are frequently referenced in the PIM BSR configuration:

- Bootstrap Router (BSR) — A BSR advertises Rendezvous Point (RP) information to other routers with PIM on a hop-by-hop basis. Among multiple Candidate-BSRs, a single BSR is chosen after an election process. The primary purpose of this Bootstrap router is to collect all Candidate-RP (C-RP) announcements in to a database called the RP-set and to periodically send this out to all other routers in the network as BSR messages (every 60 seconds).
- Bootstrap Router (BSR) messages — BSR messages are multicast to the All-PIM-Routers group with a TTL of 1. All PIM neighbors that receive these messages retransmit them (again with a TTL of 1) out of all interfaces except the one in which the messages were received. BSR messages contain the RP-set and the IP address of the currently active BSR. This is how C-RPs know where to unicast their C-RP messages.
- Candidate Bootstrap Router (C-BSR) — A device that is configured as a candidate-BSR participates in the BSR election mechanism. A C-BSR with highest priority is elected as the BSR. The highest IP address of the C-BSR is used as a tiebreaker. The BSR election process is preemptive, for example if a new C-BSR with a higher priority comes up, it triggers a new election process.
- Candidate Rendezvous Point (C-RP) — An RP acts as a meeting place for sources and receivers of multicast data. A device that is configured as a C-RP periodically advertises the multicast group mapping information directly to the elected BSR through unicast. These messages contain the Group-range, C-RP address, and a hold time. The IP address of the current BSR is learned from the periodic BSR messages that are received by all routers in the network. In this way, the BSR learns about possible RPs that are currently up and reachable.

（注） The Firewall Threat Defense device does not act as a C-RP, even though the C-RP is a mandatory requirement for BSR traffic. Only routers can act as a C-RP. So, for BSR testing functionality, you must add routers to the topology.

- BSR Election Mechanism — Each C-BSR originates Bootstrap messages (BSMs) that contain a BSR Priority field. Routers within the domain flood the BSMs throughout the domain. A C-BSR that hears about a higher-priority C-BSR than itself suppresses its sending of further BSMs for some period of time. The single remaining C-BSR becomes the elected BSR, and its BSMs inform all the other routers in the domain that it is the elected BSR.

Multicast Group Concept

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group using IGMP. Hosts must be a member of the group to receive the data stream.

Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

Clustering

Multicast routing supports clustering. In Spanned EtherChannel clustering, the control unit sends all multicast routing packets and data packets until fast-path forwarding is established. After fast-path forwarding is established, data units may forward multicast data packets. All data flows are full flows. Stub forwarding flows are also supported. Because only one unit receives multicast packets in Spanned EtherChannel clustering, redirection to the control unit is common.

マルチキャストルーティングの要件と前提条件

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Admin

Network Admin

Guidelines for Multicast Routing

Firewall Mode

Supported only in routed firewall mode. Transparent firewall mode is not supported.

IPv6

Does not support IPv6.

Multicast Group

The range of addresses between 224.0.0.0 and 224.0.0.255 is reserved for the use of routing protocols and other topology discovery or maintenance protocols, such as gateway discovery and group membership reporting. Hence, Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addresses.

Clustering

In clustering, for IGMP and PIM, this feature is only supported on the primary unit.

Additional Guidelines

- You must configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination security zone for the rule, or it cannot be applied to multicast connections during initial connection validation.
- You cannot disable an interface with PIM configured on it. If you have configured PIM on the interface (see PIM プロトコルの設定 （14 ページ）), disabling the multicast routing and PIM does not remove the PIM configuration. You must remove (delete) the PIM configuration to disable the interface.
- PIM/IGMP Multicast routing is not supported on interfaces in a traffic zone.
- Do not configure Firewall Threat Defense to simultaneously be a Rendezvous Point (RP) and a First Hop Router.
- HSRP standby IP address does not participate in PIM neighborship. Thus, if the RP router IP is routed through a HSRP standby IP address, the multicast routing does not work in Firewall Threat Defense. Hence for the multicast traffic to pass through successfully, ensure that the route for the RP address is not the HSRP standby IP address, instead, configure the route address to an interface IP address.
- For a device using virtual routing, you can configure multicast only for its global virtual router and not for its user-defined virtual router.

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 （8 ページ）。
ステップ 3 IGMP アクセスグループの設定 （10 ページ）。
ステップ 4 IGMP スタティック グループの設定 （11 ページ）。
ステップ 5 IGMP 参加グループの設定 （12 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 [**Devices** > **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 [**Devices** > **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 [**Devices** > **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、**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 **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 [**Devices** > **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、**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 （11 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 [**Devices** > **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 device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 （17 ページ）。
ステップ 5 PIM ルート ツリーの設定 （18 ページ）。
ステップ 6 PIM リクエスト フィルタの設定 （19 ページ）。
ステップ 7 マルチキャスト境界フィルタの設定 （22 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 [**Devices** > **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 [**Devices** > **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、**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 [**Devices** > **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、**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、Multicast Bidirectional 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 [**Devices** > **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、**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、**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 [**Devices** > **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、**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 [**Devices** > **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、**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、**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 [**Devices** > **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、**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 [**Devices** > **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、**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 [**Devices** > **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、**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。