セキュアIPマルチキャストの導入

内容

概要

このドキュメントでは、IPマルチキャストネットワークインフラストラクチャを保護するためのベストプラクティスに関する一般的なガイダンスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IP マルチキャスト

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、基本的な概念と用語について説明し、次のトピックについて説明します。

- 特定のプラットフォームとネットワーク全体を保護するメカニズム。
- Source Multicast(ASM)およびSource Specific Multicast(SSM)モデル
- マルチキャスト仮想プライベートネットワーク(MVPN)セキュリティ。

- Group Encrypted Transport(GET)Virtual Private Network（VPN；バーチャルプライベートネットワーク）アーキテクチャは、マルチキャストデータプレーンまたはコントロールプレーントラフィックの機密性と整合性を提供します。

用語

IPマルチキャストには、次の2つの従来のサービスモデルがあります。

1.任意の送信元マルチキャスト(ASM)

2. Source Specific Multicast(SSM)

ASMでは、受信者はInternet Group Membership Protocol(IGMP)またはMulticast Listener Discovery(MLD)メンバーシップレポートを介してグループGに参加し、グループを示します。このレポートは、任意の送信元からグループGに送信されるトラフィックを要求するため、「any source」という名前が付けられます。 これに対して、SSMでは、受信側がソースSによって定義された特定のチャネルに加入し、ソースSがグループGに送信します。これらの各サービスモデルについて、以下で詳しく説明します。

任意の送信元マルチキャスト

ASMモデルの特徴は、次の2つのプロトコルクラスです。「dense mode flood-and-prune」および「sparse mode explicit join」:

i)デンスモードのフラッドアンドプルーンプロトコル(DVMRP/MOSPF/PIM-DM)

稠密モードのプロトコルでは、ネットワーク内のすべてのルータがすべてのツリー、その送信元、および受信者を認識します。Distance Vector Multicast Routing Protocol(DVMRP)やProtocol Independent Multicast(PIM)デンスモードなどのプロトコルは、特定のツリーに対するトラフィックが不要なトポロジ部分で「プルーニング状態」を作成することによって、ネットワーク全体に「アクティブソース」情報をフラッディングし、ツリーを構築します。フラッドアンドプルーンプロトコルとも呼ばれます。Multicast Open Shortest Path First(MOSPF)では、受信側に関する情報がネットワーク全体にフラッディングされ、ツリーの構築がサポートされます。

ネットワークの一部に組み込まれたすべてのツリーが、ネットワーク内（設定されている場合は管理スコープ内）のすべてのルータで（コンバージェンスの影響を伴って）リソース使用率を常に引き起こす可能性があるため、稠密モードプロトコルは望ましくありません。 これらのプロトコルについては、この記事の残りの部分では説明しません。

（ロ）Sparse Mode Explicit Join Protocol(PIM-SM/PIM-BiDir)

スパースモードの明示的参加プロトコルでは、受信側がグループに対して明示的なIGMP/MLDメンバーシップレポート（または「参加」）を送信しない限り、デバイスはネットワーク内にグループ固有の状態を作成しません。このASMのバリアントは拡張性が高いことが知られており、マルチキャストパラダイムの焦点となります。

これがPIM-Sparseモードの基礎であり、ほとんどのマルチキャスト展開はこの時点まで使用してきました。これは、双方向PIM(PIM-BiDir)の基盤でもあります。双方向PIMは、MANY（ソース）からMANY（レシーバ）のアプリケーション向けにますます展開されています。

これらのプロトコルは、「スパースモード」のレシーバ集団を持つIPマルチキャスト配信ツリーを効率的にサポートし、送信元と受信側の間のパスにあるルータ、およびPIM-SM/BiDirではランデブーポイント(RP)でのみコントロールプレーンステートを作成するため、スパースモードと呼ばれます。 ネットワークの他の部分で状態が発生することはありません。ルータ内の状態は、下流のルータまたは受信側から参加を受信した場合にのみ明示的に構築されるため、「明示的な参加プロトコル」という名前が付けられます。

PIM-SMとPIM-BiDirは両方とも「共有ツリー」を使用し、任意の送信元からのトラフィックを受信側に転送できます。共有ツリーのマルチキャスト状態は(*,G)状態と呼ばれ、*はANY SOURCEのワイルドカードです。さらに、PIM-SMは、特定の送信元からのトラフィックに関連する状態の作成をサポートします。これらはソースツリーと呼ばれ、関連付けられた状態は(S,G)状態と呼ばれます。

Source-Specific Multicast

SSMは、受信側（または一部のプロキシ）が(S,G)「参加」を送信し、送信元Sからグループ Gに送信されたトラフィックを受信することを示すときに使用されるモデルです。これは、IGMPv3/MLDv2の「INCLUDE」モードメンバーシップレポートで可能です。このモデルは、Source-Specific Multicast(SSM)モデルと呼ばれます。SSMでは、ルータ間での明示的参加プロトコルの使用が義務付けられています。この標準プロトコルはPIM-SSMで、これは(S,G)ツリーの作成に使用されるPIM-SMのサブセットです。SSMには共有ツリー(*,G)状態はありません。

したがって、マルチキャスト受信側はASMグループGに「参加」、またはSSM(S,G)チャネルに「参加」（またはより正確には「加入」）できます。「ASMグループまたはSSMチャネル」という用語の繰り返しを避けるために、（マルチキャスト）フローという用語が使用されます。これは、フローがASMグループまたはSSMチャネルである可能性を意味します。

関連するマルチキャストプロトコル/パケットタイプ

マルチキャストネットワークを保護するには、一般的に発生するパケットの種類と、それらから保護する方法を理解することが重要です。関連するプロトコルは主に3つあります。

1. IGMP/MLD
2. PIM
3. MSDP

次のセクションでは、これらの各プロトコルについて説明し、各プロトコルで発生する可能性のある問題について説明します。

IGMP/MLDパケット

IGMP/MLDは、マルチキャスト受信者が特定のマルチキャストグループのコンテンツを受信する必要があることをルータに通知するために使用するプロトコルです。Internet Group Membership Protocol(IGMP)はIPv4で使用されるプロトコルで、Multicast Listener Discovery(MLD)はIPv6で使用されるプロトコルです。

IGMPには、IGMPv2とIGMPv3の2つのバージョンが一般的に導入されています。また、MLDには、MLDv1とMLDv2の2つのバージョンが一般的に導入されています。

IGMPv2とMLDv1は機能的に同等で、IGMPv3とMLDv2は機能的に同等です。

これらのプロトコルは、次のリンクで指定されます。

IGMPv2:RFC 2236

MLDv1:RFC 3590

IGMPv3およびMLDv2:RFC 4604

IGMPv2とIGMPv3はプロトコルであるだけでなく、IPv4 IPプロトコル（具体的にはプロトコル番号2）でもあります。 これらのRFCで説明されているように、マルチキャストグループメンバーシップを報告するためだけでなく、DVMRP、PIMバージョン1、mtrace、mrinfoなどの他のIPv4マルチキャストプロトコルでも使用されます。これは、IGMPをフィルタリングする際に(Cisco IOS® ACLなどを使用して)覚えておくことが重要です。 IPv6では、MLDはIPv6プロトコルではありません。代わりに、MLDパケットの伝送にICMPv6が使用されます。PIMバージョン2は、IPv4とIPv6（プロトコル番号103）で同じプロトコルタイプです。

PIM制御パケット

このセクションでは、マルチキャストおよびユニキャストPIM制御パケットについて説明します。Auto-RPとBootstrap Router（BSR；ブートストラップルータ）について説明します。BSRは、PIM-SMネットワークでランデブーポイントを選択し、グループ間の割り当てを制御する方法です。

マルチキャストPIM制御パケット

マルチキャストPIM制御パケットには次のものがあります。

- **PIM Hello**:PIM Helloパケットは、PIMネイバーを確立するために同じネットワークに接続されたルータに送信される、リンクローカルスコープのIPマルチキャストパケットです。
- **PIM Join/Prune**:PIM Join/Pruneは、マルチキャスト状態を作成/削除するために送信されるリンクローカルスコープIPマルチキャストパケットで、PIMネイバーにのみ送信されます。これらはアサート、レポート抑制、およびその他のPIMプロトコルの詳細を容易にするためにLAN内のマルチキャストですが、常に特定のネイバーに送信されます。
- **PIM DF-elect**:PIM指定フォワーダは、接続されたレシーバまたはダウンストリームPIMネイバーに代わってRPに送信される(*,G)JOINを処理するBi-Dir PIMルータです。PIMルータが、同じグループGの同じセグメントで(*,G) JOINを送信する別のルータを検出した場合、RPへのベストパスを持つルータを決定する選択があります。
- **PIM Assert**:PIMアサートは、特定のインターフェイスから特定の(S、G)のパケットをアクティブに転送するネットワークセグメントに接続されたPIMルータが、転送される同じインターフェイスでその同じ(S、G)のパケットの受信を開始したときに送信されるリンクローカルIPマルチキャストパケットです。このイベントは、この(S,G)のシングルフォワーダ(SF)と見なされる別のルータが存在することを示します。 アサートメカニズムは、その(S,G)に対して一意のSFを選択します。 PIM SFルータは、特定の(S,G)ストリームのパケットを転送するよ

うに選択されます。PIMでは、異なるルータが異なる(S,G)の代わりにSFの役割を実行できます。理想的には、(S,G)ごとに1つのSFしかありません。 SFと代表ルータを混同しないでください。PIM代表ルータは、PIM-SMネットワークのRPに送信されるJOIN/PRUNESまたはSOURCE REGISTERSを担当するルータです。
- **PIMブートストラップ**:PIMブートストラップメッセージがPIMv2ネットワークで送信され、特定のグループGに対するランデブーポイントの動的な選択を容易にします。

ユニキャストPIM制御パケット

ユニキャストPIM制御パケットは、RPに対して送受信され、次の内容が含まれます。

- **Source Register Packet**：ランデブーポイントに新しいマルチキャストソースを登録するためにPIMソースレジスタパケットが送信されます。送信元がマルチキャストパケットの送信を開始すると、送信元ネットワークに接続されている代表ルータ(DR)は、RPにユニキャストレジスタストリームを送信して、RPが担当するマルチキャストグループにアクティブな送信元があることを示します。
  送信元レジスタパケットは、元のマルチキャストストリームのユニキャストカプセル化として送信されます。
  PIMレジスタメッセージはプロセスレベルでスイッチングされ、RPがレジスタ停止メッセージを送信するまで送信されます。これらのパケットのパフォーマンスへの影響は、送信元のレート((S,G)フローごと)に比例します。
- **Register Stop Packet**:PIM Register Stop PacketsがランデブーポイントからRegisterメッセージを送信したPIM DRに送信されます。Register Stopメッセージは、RPが送信元からのマルチキャストパケットのネイティブな受信を開始するとすぐに送信されます。
- **BSR Candidate-Rendezvous Point Advertisement Packet**:PIM BSR C-RP-Advertisement Packetは、BSRが選出されるとBSRに送信され、RP候補がアドバタイズされます。

図 1：PIMユニキャストパケット

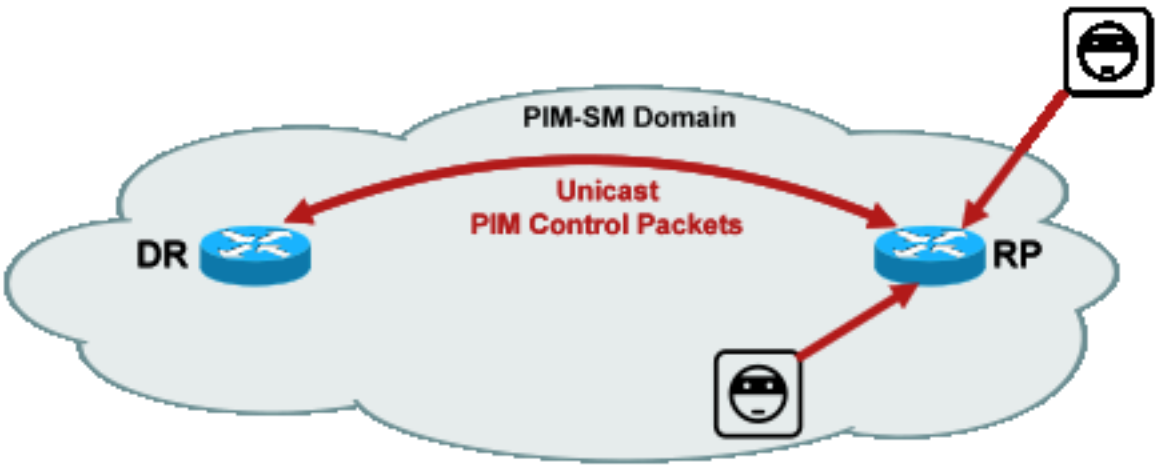

Fig1

_PIM_unicast

これらのパケットはユニキャストであるため、このようなパケットを悪用する攻撃はどこからでも発生する可能性があります。

Auto-RPパケット

Auto-RPは、PIMv2 BSRと同じ目的で動作するシスコが開発したプロトコルです。Auto-RPはBSRより前に開発されており、IPv4のみをサポートします。BSRはIPv4とIPv6をサポートします。Auto-RPのMapping Agentは、BSRのブートストラップルータと同じ機能を提供します。BSRでは、C-RPからのメッセージはブートストラップルータにユニキャストされます。Auto-RPでは、メッセージはマルチキャストを介してマッピングエージェントに送信されます。これにより、後で説明するように、境界でのフィルタが容易になります。Auto-RPの詳細については、次のリンクを参照してください。
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Cisco IOSでは、AutoRP/BSRパケットは常に転送され、現在は無効になっていません。これは、Auto-RPの場合、特定のセキュリティ上の問題を引き起こす可能性があります。

図 2：Auto-RPパケット

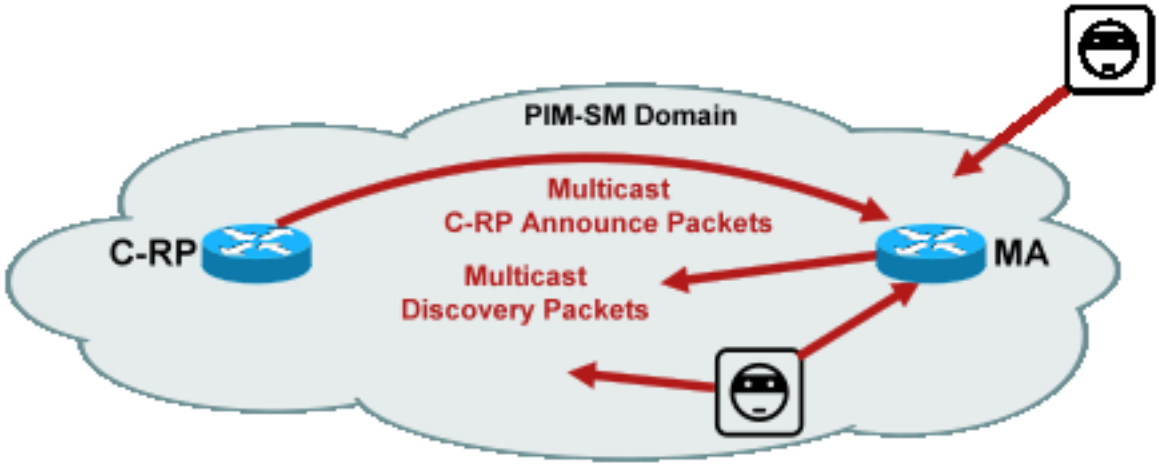

fig2_Au

toRP_packets

注：Auto-RPはPIM-SM RPのアナウンスとディスカバリのメカニズムとして使用されますが、PIMパケットを使用しません（IPプロトコル103）。代わりに、マルチキャストアドレスを持つユーザデータグラムプロトコル(UDP)ポート496パケットを使用します。

Auto-RPで使用されるパケットタイプには、次の2つがあります。

- C-RP-Announceパケット：これらのパケットはすべてのマッピングエージェントに対してマルチキャストされ、Internet Assigned Numbers Authority(IANA)によって予約された「既知の」アドレス(224.0.1.39)を使用します。 これらはC-RPによって送信され、RPアドレスと、そのRPがRPとして動作できるグループ範囲をアナウンスします。
- C-RPディスカバリパケット：これらのパケットはすべてのPIMルータに対してマルチキャストされ、IANAによって予約された「既知の」アドレス(224.0.1.40)を使用します。 これらはAuto-RPマッピングエージェントによって送信され、特定のグループ範囲のRPとして選択された特定のC-RPをアナウンスします。

これらのパケットタイプはそれぞれ、ネットワークを通じてフラッディングされることを意図しています。

Cisco IOSでは、グループがRP情報の配布に使用される場合、そのグループに関するRPの事前知識がないという問題を回避するために、224.0.1.39と224.0.1.40の両方がPIMデンスモードで転送されます。これは、PIMデンスモードの唯一の推奨用途です。

Cisco IOS XRでは、Auto-RPメッセージは、Reverse Path Forwarding(RPF)によってネイバーからネイバーにホップ単位でフラッディングされます。したがって、Cisco IOS XRでAuto-RPをサポートするためにPIM DM mroute状態を作成する必要はありません。実際、Cisco IOS XRはPIM-DMをまったくサポートしていません。

Multicast Service Discovery Protocol(MSDP)パケット

MSDPは、あるドメインの送信元を、それぞれのランデブーポイントを介して別のドメインの受信者にアナウンスできるようにするIPv4プロトコルです。MSDPはRFC 3618で指定されています。

PIMドメイン間でアクティブなソースに関する情報を共有するには、MSDPが使用されます。あるドメインで送信元がアクティブになった場合、MSDPにより、すべてのピアドメインがこの新しい送信元についてタイムリーに学習するようになります。これにより、他のドメインの受信者は、受信者が関心を持つグループに送信した場合に、この新しい送信元とすばやく連絡を取ることができます。MSDPはASM/PIM-SMマルチキャスト通信に必要で、各ドメインのランデブーポイント間に設定されたユニキャストTransport Control Protocol(TCP)接続で実行されます。

マルチキャスト環境における脅威

信頼境界のゾーン

ドキュメントのこのセクションは、ネットワーク内の機能エンティティ別にまとめられています。ここで説明する脅威モデルは、これらのエンティティを中心に形成されています。たとえば、このドキュメントでは、ルータの配置場所に関係なく、マルチキャストネットワーク内のルータを（マルチキャストの観点から）保護する方法について説明します。同様に、ネットワーク全体のセキュリティ対策、または代表ルータやランデブーポイントでの対策の導入方法についても考慮する必要があります

ここで説明する脅威もこのロジックに従い、ネットワーク内の論理機能別に整理されます。

脅威の概要

抽象的なレベルでは、あらゆるマルチキャスト展開が、セキュリティのさまざまな側面に関する多数の脅威の対象となる可能性があります。セキュリティの重要な側面は、機密性、整合性、可用性です。

- **機密性に対する脅威**:ほとんどのアプリケーションでは、マルチキャストトラフィックは暗号化されないため、パス内の任意の回線またはネットワーク要素でリッスンまたはキャプチャを行うために誰にでもオープンです。このような攻撃を防ぐためにマルチキャストトラフィックを暗号化する方法については、「GET VPN」の項を参照してください。

- **トラフィックの完全性に対する脅威**:アプリケーションレベルのセキュリティや、GET VPNなどのネットワークベースのセキュリティがなければ、マルチキャストトラフィックは送信中に変更される可能性があります。これは、OSPF、PIM、その他多くのプロトコルなど、マルチキャストを使用するコントロールプレーントラフィックにとって特に重要です。
- **ネットワークの完全性に対する脅威**:このドキュメントで説明されているセキュリティメカニズムがないと、不正な送信者、受信者、または侵害されたネットワーク要素がマルチキャストネットワークにアクセスし、許可なしでトラフィックを送受信したり（サービスの盗難）、ネットワークリソースを過負荷状態にしたりする可能性があります。
- **可用性に対する脅威**:正当なユーザがリソースを利用できないようにするために、サービス拒否攻撃の可能性が数多くあります。

次のセクションでは、ネットワーク内の各論理機能の脅威について説明します。

ルータに対する基本的な脅威

ルータに対しては、ルータがマルチキャストをサポートするかどうか、および攻撃にマルチキャストトラフィックやプロトコルが含まれるかどうかとは無関係に、いくつかの基本的な脅威があります。

サービス拒否(DoS)攻撃は、ネットワークにおける最も重要な一般的な攻撃ベクトルです。原則的に、すべてのネットワーク要素がDoS攻撃の対象となり、正当なユーザのサービスが失われたり劣化したりする可能性があるため、要素が過負荷になる可能性があります。ユニキャストに適用される基本的なネットワークセキュリティの推奨事項に従うことは最も重要です。

マルチキャスト攻撃は必ずしも意図的なものではなく、偶発的であることが多いことは注目に値します。たとえば、2004年3月に初めて観察されたWittyワームは、IPアドレスに対するランダムな攻撃によって広がったワームの一例です。アドレス空間が完全にランダム化された結果、マルチキャストIP宛先もこのワームの影響を受けました。多くの組織では、ワームが多数の異なるマルチキャスト宛先アドレスにパケットを送信したため、多数のファーストホップルータがクラッシュしました。しかし、ルータは、関連するステートの作成に伴うマルチキャストトラフィックの負荷の範囲が設定されておらず、リソースの枯渇を効果的に経験していました。これは、マルチキャストが企業で使用されていない場合でも、マルチキャストトラフィックを保護する必要性を示しています。

ルータに対する一般的な脅威は次のとおりです。

- パケットフラッドのタイプは問いません。たとえば、低速（パント）パスなどのハードウェアパスや、Secure Shell(SSH)、Telnet、Border Gateway Protocol(BGP)、OSPF、Network Time Protocol(NTP)などを含む管理またはコントロールプレーンポートなどのソフトウェアパスに対して使用します
- ルータへの侵入とその後のルータ機能の不正利用現在のネットワークでは、TelnetまたはSSHのパスワードが弱く、Simple Network Management Protocol(SNMP)コミュニティストリングが弱いことが一般的な問題です。
- 設定ミスやインサイダー攻撃などの運用上の問題は、ネットワーク全体とそのトラフィックのセキュリティを危険にさらす可能性があります。

ルータでマルチキャストを有効にする場合は、ユニキャストに加えてマルチキャストも保護する必要があります。IPマルチキャストを使用しても、基本的な脅威モデルは変わりません。ただし、攻撃を受ける可能性のある追加プロトコル(PIM、IGMP、MLD、MSDP)を有効にするので、特に保護する必要があります。これらのプロトコルでユニキャストトラフィックが使用される場合、脅威モデルはルータで実行される他のプロトコルと同じです。

マルチキャストトラフィックは基本的に「受信者主導」であり、リモートの宛先を対象とすることはできないため、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と同じように使用してルータを攻撃することはできません。攻撃ターゲットは、マルチキャストストリームに明示的に「参加」する必要があります。ほとんどの場合（Auto-RPが主な例外です）、ルータは「リンクローカル」マルチキャストトラフィックをリッスンして受信するだけです。リンクローカルトラフィックは転送されません。したがって、マルチキャストパケットを含むルータに対する攻撃は、直接接続された攻撃者からのみ発生します。

送信元からの脅威

マルチキャストソース（PCまたはビデオサーバがネットワークと同じ管理制御下にない場合があります）。したがって、送信者はネットワークオペレータの観点からは、ほとんどの場合、信頼できないと見なされます。PCとサーバの強力な機能と、しばしば不完全な複雑なセキュリティ設定を考えると、送信者はマルチキャストを含むあらゆるネットワークに対して重大な脅威を提起します。これらの脅威には次のものがあります。

- **レイヤ2攻撃**：レイヤ2にはさまざまな攻撃形式があり、さまざまな種類の攻撃を実行できます。これらはマルチキャストだけでなくユニキャストにも適用されます。これらの攻撃形式はマルチキャストに固有のものではないため、このドキュメントでは詳細に説明しません。詳細については、Cisco Pressの書籍『LAN Switch Security』(ISBN-10:1-58705-467-1.
- **マルチキャストトラフィックによる攻撃**：前述したように、ファーストホップルータはグループのリスナーがない限りマルチキャストトラフィックを転送しないため、マルチキャストトラフィックによる攻撃は困難です。ただし、マルチキャストパケットを使用して、ファーストホップをさまざまな方法で攻撃できます。
- ネットワーク飽和攻撃：攻撃者は、使用可能な帯域幅を使用してセグメントをマルチキャストパケットでフラッディングし、DoS状態を引き起こす可能性があります。
- マルチキャスト状態攻撃：ファーストホップルータはマルチキャストパケットでフラッディングされるため、状態が過剰になり、結果としてDoS攻撃状態が発生する可能性があります。
- 送信側は、送信されたPIM helloを通じてPIM DRになろうとします。このような場合、LANとの間でトラフィックが転送されることはありません。
- BiDir-PIM DFのPIM DF選択パケットがスプーフィングされる可能性がある。このような場合、LANとの間でトラフィックが転送されることはありません。
- 送信側は、AutoRP RPディスカバリまたはBSRブートストラップメッセージをスプーフィングする可能性があります。これは実際には偽のRPをアナウンスし、PIM-SM/BiDirサービスを停止または中断させます。
- 送信者は、PIMソースレジスタ/レジスタ停止メッセージなどのユニキャスト攻撃を送信したり、BSRアナウンスパケットを送信して偽のBSRをアナウンスしたりできます。
- 送信者は、フィルタリングされていない限り、任意の有効なマルチキャストグループに送信

できます。送信元アドレスがスプーフィングされ、エッジで阻止されない場合、送信者は正当な送信者の送信元IPアドレスを使用し、ネットワークの一部のコンテンツを上書きできます。
- コントロールプレーンプロトコルに対するマルチキャスト攻撃：OSPFやDynamic Host Configuration Protocol（DHCP；ダイナミックホストコンフィギュレーションプロトコル）など、マルチキャストに関連付けられていないプロトコルの多くは、マルチキャストパケットを使用します。このパケットを使用してこれらのプロトコルを攻撃できます
- **Masquerading：送**信者が別の送信者のふりをできる攻撃形態は数多くあります。スプーフィングされた送信元IPアドレスは、このような攻撃の形態の1つです。
- **サービスの盗用：送**信側が制御されない限り、送信側から不正にマルチキャストサービスを使用できます。

注：通常、ホストはPIMパケットを送受信しません。これを行うホストは、攻撃を試みる可能性があります。

受信側からの脅威

レシーバは通常、CPUパワーと帯域幅が大きいプラットフォームでもあり、さまざまな攻撃形式に対応できます。これらは、送信側の脅威とほぼ同じです。レイヤ2攻撃は、依然として重要な攻撃ベクトルです。偽のレシーバとサービスの盗用もレシーバ側で可能ですが、攻撃ベクトルは通常IGMP（または前述したようにレイヤ2攻撃）です。

ランデブーポイントおよびBSRに対する脅威

PIM-SM RPとPIM-BSRはマルチキャストネットワークの重要なポイントであるため、攻撃者の重要なターゲットとなります。どちらのルータもファーストホップルータではない場合は、PIMユニキャストを含むユニキャスト攻撃形式だけをこれらの要素に対して直接標的にすることができます。RPおよびBSRに対する脅威には次のものがあります。

- 「ルータに対する基本的な脅威」の項で説明されている、すべての一般的な攻撃形式。
- スプーフィングされた送信元IPアドレスを使用する可能性のあるPIMユニキャスト攻撃では、悪意のあるデバイスから送信されるPIMレジスタメッセージまたはレジスタストップメッセージを介して、DoS攻撃が可能になります。

マルチキャストおよびユニキャストセキュリティ（比較）

状態に関する考慮事項/フィルタ

図3のトポロジを考えてみます。このトポロジには、送信元、3つの受信側(A、B、C)、スイッチ(S1)、および2つのルータ（R1とR2）が示されています。 青い線はユニキャストストリームを表し、赤い線はマルチキャストストリームを表します。3つのレシーバはすべてマルチキャストフローのメンバーです。

図 3：ルータおよびスイッチでの複製

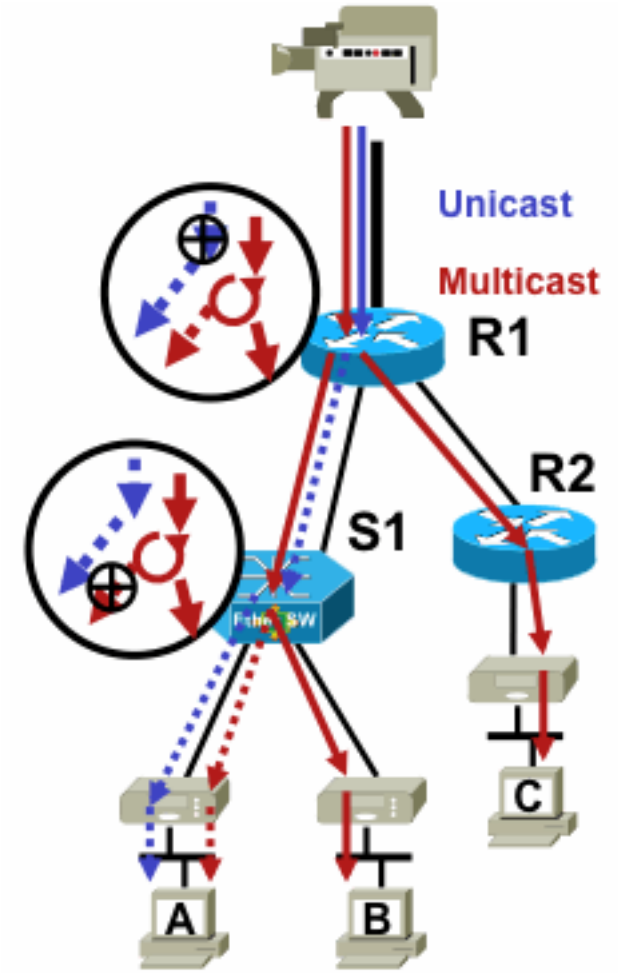

fig3_replication_RS

特定の送信元から特定の受信者へのトラフィックフローを抑制するには、次の手順を実行します。

- ユニキャストストリームの場合は、送信者から受信者までのパス上の任意の場所にフィルタをインストールします。
- ただし、マルチキャストストリームの場合、管理者はフィルタをインストールする場所をより具体的に指定する必要があります。受信側で、受信側の直前のレプリケーションポイントの後にフィルタを実行します。ソース側のフィルタで、ソースの後の最初のレプリケーションポイントの前に配置します。

マルチキャスト送信元からの攻撃

この項は、ASMおよびSSMの両方のサービスモデルに適用されます。これらのサービスモデルでは、トラフィックは受信側の明示的な加入の受信に基づいて転送されます。

ユニキャストストリームの場合、暗黙的なレシーバ保護はありません。ユニキャスト送信元は、宛先がトラフィックを要求していない場合でも、その宛先にトラフィックを送信できます。そのため、ファイアウォールなどの防御メカニズムは通常、エンドポイントを保護するために使用されます。一方、マルチキャストには、プロトコルに組み込まれた暗黙の保護があります。トラフィックは、問題のフローに参加している受信者にのみ到達するのが理想的です。

ASMを使用すると、送信元は、アクティブなRPでサポートされている任意のグループへのマルチキャストトラフィック伝送を通じて、トラフィック挿入またはDoS攻撃を開始できます。このトラフィックは理想的には受信側には到達しませんが、少なくともパス内のファーストホップルータやRPに到達できます。これにより、限定的な攻撃が可能になります。ただし、悪意のある送信元がターゲット受信者が対象とするグループを知っていて、適切なフィルタが設定されていない場合、そのグループにトラフィックを送信できます。このトラフィックは、レシーバがグループをリッスンしている限り受信されます。

SSMでは、受信側がその(S,G)チャネルに参加していない場合にトラフィックが停止するファーストホップルータでのみ、不要な送信元による攻撃が可能です。ファーストホップルータは、明示的な加入状態が存在しないSSMトラフィックをすべて受信側から廃棄するため、この攻撃によるファーストホップルータへの状態攻撃は発生しません。このモデルでは、「結合」はソース固有であるため、悪意のあるソースがターゲットが関心のあるグループを知るだけでは十分ではありません。ここでは、スプーフィングされたIP送信元アドレスと潜在的なルーティング攻撃が成功に必要です。

状態攻撃

ネットワーク内にレシーバが存在しない場合でも、PIM-SMは送信元に最も近いファーストホップルータとランデブーポイントに(S,G)および(*,G)状態を作成します。したがって、送信元のファーストホップルータとPIM-SM RPのネットワークで状態攻撃が発生する可能性があります。

悪意のある送信元が複数のグループにトラフィックを送信し始めた場合、RPの設定で問題のグループが許可されていれば、検出されたグループごとに、ネットワーク内のルータが送信元とRPで状態を作成します。

したがって、PIM-SMは送信元による状態およびトラフィック攻撃の対象となります。送信元が正しいプレフィクス内で送信元IPアドレスをランダムに変更した場合、つまりアドレスのホストビットだけがスプーフィングされた場合、この攻撃は悪化する可能性があります。

図 4：ASM RP攻撃

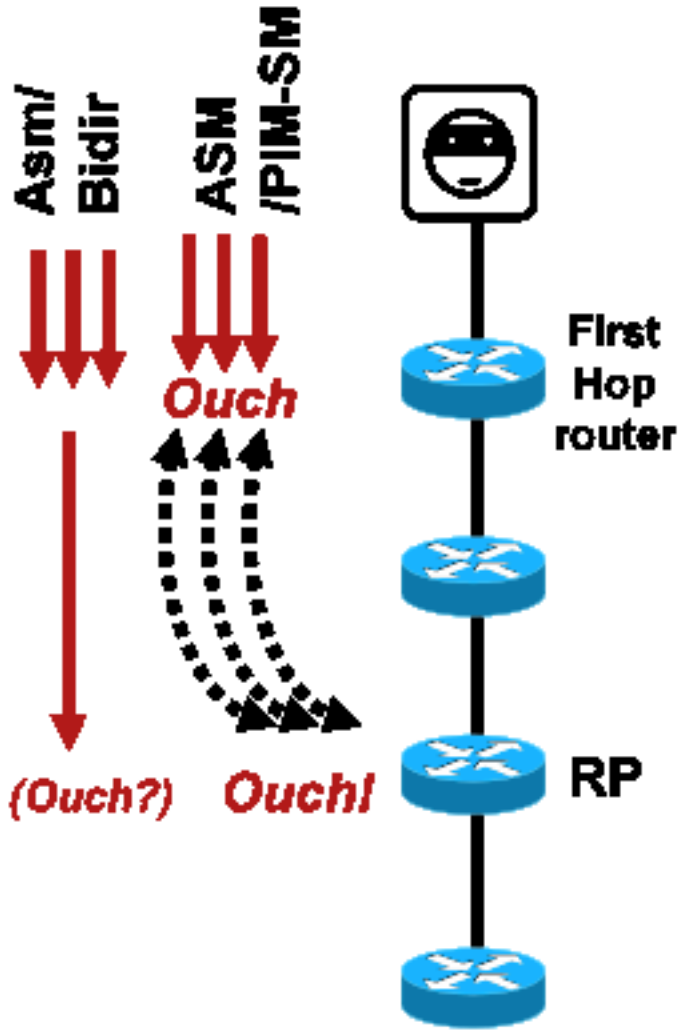

fig4_ASM_RP_Attacks

PIM-SSMと同様に、送信元からのPIM-BiDir状態生成攻撃は不可能です。PIM-BiDir内のトラフィックは、RPに対して状態が転送されるだけでなく、受信側からのJoinによって作成された状態でも転送されます。これにより、JoinはRPにしか到達しないため、RPの背後にある受信側に到達できるようになります。RPへのステートツーフォワードトラフィックは(*,G/M)ステートと呼ばれ、RP設定（スタティック、Auto-RP、BSR）によって作成されます。 ソースの存在が変わることはありません。したがって、攻撃者はマルチキャストトラフィックをPIM-BiDir RPに送信できますが、PIM-SMとは異なり、PIM-BiDir RPは「アクティブ」なエンティティではなく、PIM-BiDirグループのトラフィックを転送または廃棄するだけです。

> **注**：一部のCisco IOSプラットフォーム(*,G/M)では、状態がサポートされていません。このような場合、送信元は複数のPIM-BiDirグループにマルチキャストトラフィックを送信することでルータを攻撃し、(*,G)状態を作成する可能性があります。たとえば、Catalyst 6500スイッチは(*,G/M)状態をサポートしています。

受信者による攻撃

攻撃はマルチキャスト受信側から発生する可能性があります。通常、IGMP/MLDレポートを送信する受信側は、ファーストホップルータ上で状態を作成します。ユニキャストには、これに相当するメカニズムはありません。

図 5：受信側の明示的な参加ベースのトラフィック転送

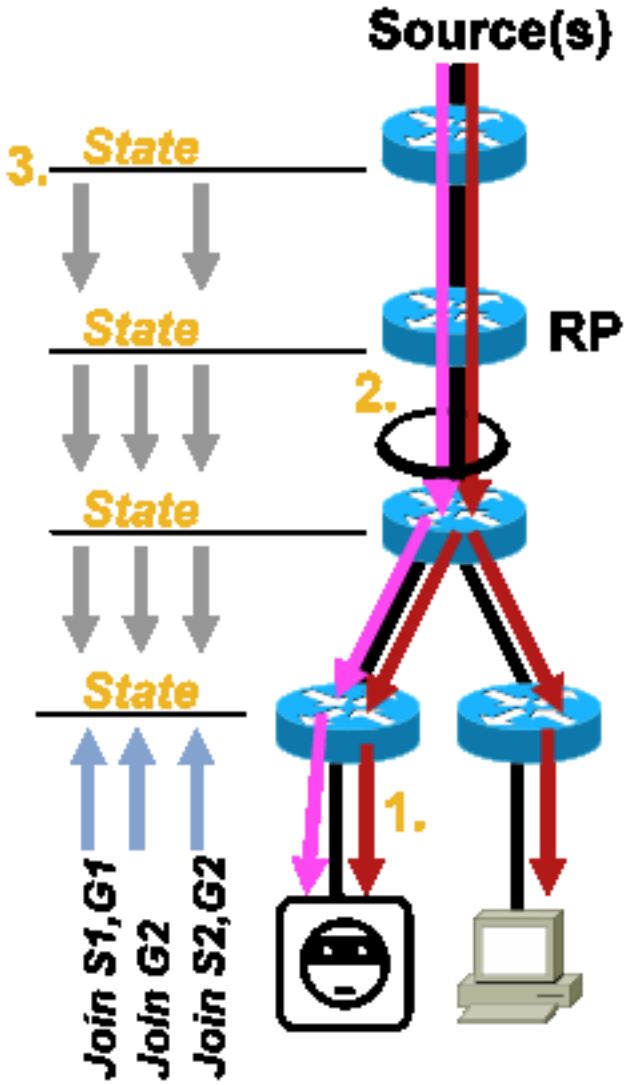

Fig5_Receiver_Explicit_Join

レシーバ攻撃には、次の3つのタイプがあります。

1. マルチキャスト受信者は、許可されていないフローへの参加を試みたり、許可されていないコンテンツの受信を試みたりできます。
2. マルチキャスト受信側は、多くのグループまたはチャネルに関心を持たせることで、使用可能なネットワーク帯域幅を過負荷にする可能性があります。この種の攻撃は、他の潜在的なコンテンツの受信者に対する共有帯域幅攻撃になります。
3. マルチキャスト受信側は、ルータまたはスイッチに対する攻撃を試みることができます。大量のIGMPレポートを生成できるため、大量のマルチキャストツリー状態が発生し、ルータのキャパシティが過負荷になる可能性があります。その結果、マルチキャストコンバージェンス時間が増加したり、ルータのDoSが増加したりする可能性があります。

次のセクション「マルチキャストネットワーク内のセキュリティ」では、このような攻撃を軽減するさまざまな方法について説明します。

マルチキャストネットワーク内のセキュリティ

ネットワークエレメントセキュリティ

セキュリティは重要な機能ではなく、すべてのネットワーク設計に不可欠な要素です。そのため、ネットワークのすべてのポイントでセキュリティを考慮する必要があります。すべてのネットワーク要素を適切に保護することが最も重要です。あらゆるテクノロジーに適用できる攻撃シナリオの1つに、侵入者によって破壊されたルータがあります。侵入者がルータを制御すると、攻撃者はさまざまな攻撃シナリオを実行できます。したがって、各ネットワーク要素は、あらゆる形式の基本攻撃に対して、また特定のマルチキャスト攻撃に対しても適切に保護する必要があります。

コントロール プレーン ポリシング（CoPP）

CoPPはルータACL(rACL)の進化であり、ほとんどのプラットフォームで使用できます。原則は同じです。ルータ宛てのトラフィックだけがCoPPによってポリシングされます。

サービスポリシーは、ポリシーマップとクラスマップを使用して、あらゆるQuality of Service(QoS)ポリシーと同じ構文を使用します。そのため、コントロールプレーンに向かう特定のトラフィックに対するレートリミッタを使用して、rACL（許可/拒否）の機能を拡張します。

> **注**：Catalyst 9000シリーズスイッチなどの特定のプラットフォームでは、CoPPがデフォルトで有効になっており、保護は置き換えられません。詳細については、『CoPPガイド』を参照してください。

実稼働中のネットワークでrACLまたはCoPPを調整、変更、または作成する場合は、注意が必要です。どちらの機能もコントロールプレーンへのすべてのトラフィックをフィルタリングする機能を備えているため、必要なすべてのコントロールプレーンプロトコルと管理プレーンプロトコルを明示的に許可する必要があります。必要なプロトコルのリストは大きく、Terminal Access Controller Access Control System(TACACS)など、あまり目立たないプロトコルは見逃しやすい場合があります。 デフォルト以外のすべてのrACLおよびCoPP設定は、実稼働ネットワークに導入する前に、必ずラボ環境でテストする必要があります。さらに、初期導入は「許可」ポリシーのみで開始する必要があります。これにより、ACLヒットカウンタを使用して予期しないヒットを検証できます。

マルチキャスト環境では、マルチキャストが正しく機能するために、必要なマルチキャストプロトコル（PIM、MSDP、IGMPなど）がrACLまたはCoPPで許可されている必要があります。PIM-SMのシナリオでは、送信元からマルチキャストストリームの最初のパケットがコントロールプレーンパケットとして使用され、デバイスのコントロールプレーンでマルチキャスト状態を作成するのに役立ちます。したがって、rACLまたはCoPPで関連するマルチキャストグループを許可することが重要です。プラットフォーム固有の例外が多数あるため、展開の前に関連するドキュメントを参照し、計画されている設定をテストすることが重要です。

ローカルパケットトランスポートサービス(LPTS)

Cisco IOS XRでは、Local Packet Transport Service(LPTS)が、Cisco IOSのCoPPと同様に、ルータのコントロールプレーンへのトラフィックのポリサーとして機能します。さらに、ユニキャス

トおよびマルチキャストトラフィックを含む受信トラフィックをフィルタリングし、レートを制限できます。

マルチキャスト固有のセキュリティ

マルチキャスト対応ネットワークでは、各ネットワーク要素はマルチキャスト固有のセキュリティ機能で保護する必要があります。一般的なルータ保護については、このセクションで説明します。すべてのルータに必要ない機能ですが、ネットワーク内の特定の場所にのみ必要な機能、およびルータ間の相互対話を必要とする機能（PIM認証など）については、次のセクションで説明します。

Mroute制限

mroute limitコマンドは、ルータ上のマルチキャストルートの量をグローバルに制限し、DoS攻撃の防止に役立ちます。

ip multicast route-limit <mroute-limit> <warning-threshold>

図 6：Mroute制限

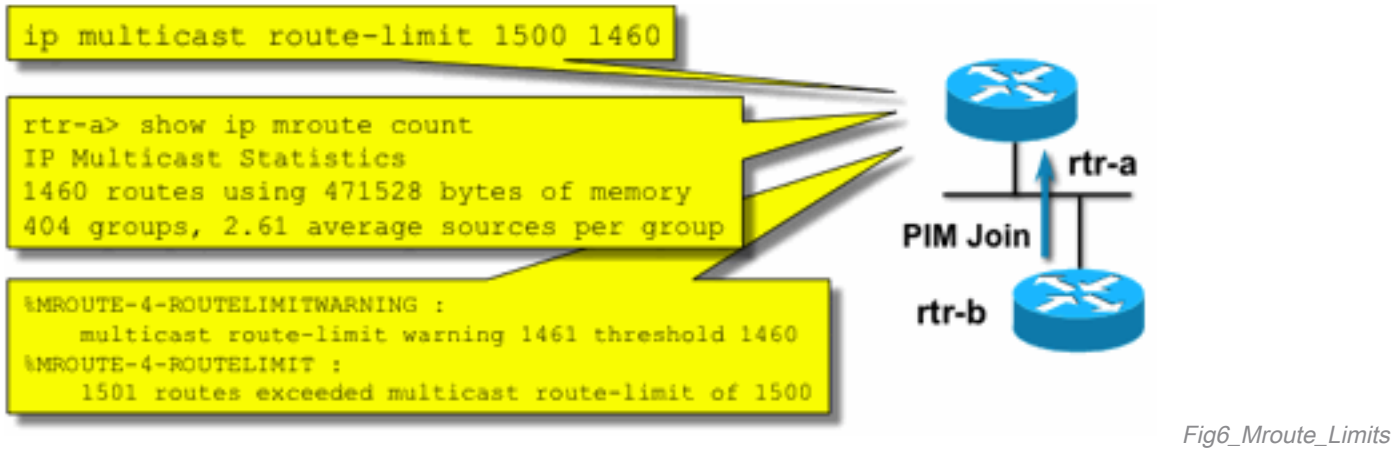

Fig6_Mroute_Limits

Mrouteの制限により、マルチキャストルーティングテーブルへのmrouteの許可数のしきい値を設定できます。マルチキャストルートの制限が有効になっている場合、設定された制限を超えるマルチキャスト状態は作成されません。警告のしきい値もあります。mrouteの数が警告のしきい値を超えると、syslog警告メッセージがトリガーされます。mroute制限では、状態を引き起こすそれ以上のパケットは廃棄されます。

ip multicast route-limitコマンドは、MVRF単位でも使用できます。

SAPリッスンの無効化：no ip sap listen

sap listenコマンドにより、ルータはSession Announcement Protocol/Session Description Protocol(SAP/SDP)メッセージを受信します。SAP/SDPは、マルチキャストバックボーン(MBONE)の時代から始まるレガシープロトコルです。 これらのメッセージは、将来または現時点で利用可能なマルチキャストコンテンツに関するディレクトリ情報を示します。これは、ルータのCPUおよびメモリリソースに対するDoSの原因となる可能性があるため、この機能を無効にする必要があります。

mrinfo情報へのアクセスの制御：「ip multicast mrinfo-filter」コマンド

mrinfoコマンド（Cisco IOSおよび一部のバージョンのMicrosoft WindowsとLinuxでも使用可能）は、さまざまなメッセージを使用してマルチキャストルータに情報を照会します。**ip multicast mrinfo-filter**グローバル設定コマンドを使用すると、この情報へのアクセスを送信元のサブセットに制限したり、情報を完全に無効にすることができます。

次の例では、192.168.1.1から送信されたクエリを拒否し、他の任意のソースからのクエリを許可しています。

```
ip multicast mrinfo-filter 51

access-list 51 deny 192.168.1.1
access-list 51 permit any
```

この例では、 *mrinfo* 任意のソースからの要求：

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

> **注**：予想されるとおり、*deny*はパケットがフィルタリングされることを意味し、*permit*はパケットが許可されることを意味します。

mrinfoコマンドが診断目的で使用される場合、適切なACLを使用してip multicast mrinfo-filterコマンドを設定し、送信元アドレスのサブセットからのクエリーのみを許可することを強く推奨します。*mrinfo*コマンドで提供される情報は、SNMPを介して取得することもできます。mrinfo要求の完全なブロック（デバイスのクエリからのすべてのソースをブロックする）を強く推奨します。

ネットワーク セキュリティ

このセクションでは、PIMマルチキャストおよびユニキャスト制御パケットを保護するさまざまな方法と、Auto-RPおよびBSRについて説明します。

マルチキャストグループの無効化

ip multicast group-range/ipv6 multicast group rangeコマンドを使用すると、ACLによって拒否されたグループのすべての操作を無効にできます。

```
ip multicast group-range <std-acl>
ipv6 multicast group-range <std-acl>
```

ACLによって拒否されたグループのいずれかに対してパケットが現れると、PIM、IGMP、MLD、MSDPなどのすべての制御プロトコルで廃棄され、データプレーンでも廃棄されます。したがって、これらのグループ範囲に対してIGMP/MLDキャッシュエントリ、PIM、Multicast Routing Information Base(RIB)/Multicast Forwarding Information Base(MFIB)状態が作成されず、すべてのデータパケットが即座に廃棄されます。

これらのコマンドは、デバイスのグローバルコンフィギュレーションで入力します。

ネットワーク外から発信されるすべてのマルチキャストトラフィックが制御されるように、このコマンドをネットワーク内のすべてのルータに、利用可能な場合は可能な場所で展開することを推奨します。これらのコマンドは、データプレーンとコントロールプレーンに影響することに注意してください。このコマンドを使用できる場合は、標準ACLよりも広範なカバレッジが提供されるため、このコマンドを使用することをお勧めします。

PIMセキュリティ

PIMネイバー制御

PIMネイバーシップを確立するには、PIMルータがPIM Helloを受信する必要があります。PIMネイバーシップは、代表ルータ(DR)選出、DRフェールオーバー、およびPIM Join/Prune/Assertメッセージの送受信の基礎でもあります。

図 7：PIMネイバー制御

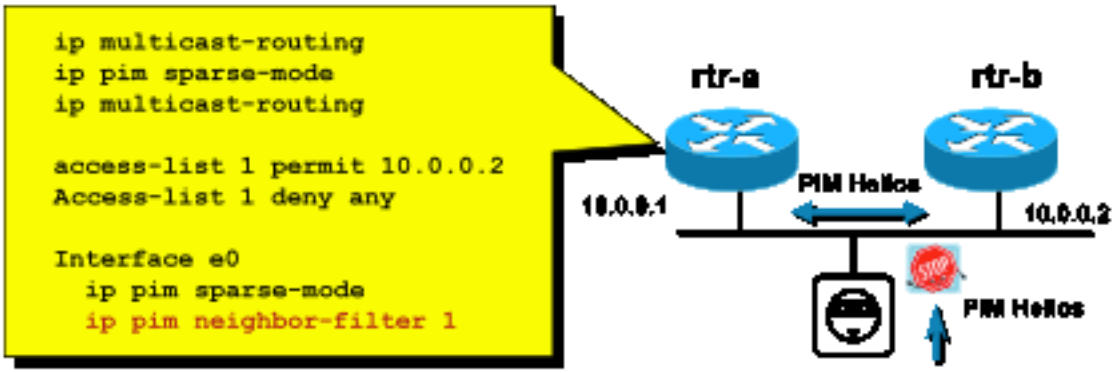

Fig7_PIM_neighbor_control

不要なネイバーを禁止するには、 **ip pim neighbor-filter** コマンドを図7に示します。このコマンドは、Hello、Join/Pruneパケット、およびBSRパケットを含むすべての非許可ネイバーPIMパケットをフィルタリングします。セグメント上のホストは、送信元IPアドレスをスプーフィングして、PIMネイバーを装う可能性があります。セグメントでの送信元アドレスのスプーフィングを防ぐため、またはアクセススイッチでVLAN ACLを使用してホストからのPIMパケットを防ぐために、レイヤ2セキュリティメカニズム（つまりIPソースガード）が必要です。キーワード「log-input」をACLで使用すると、ACEに一致するパケットをログに記録できます。

PIM Join/PruneパケットはPIMネイバーに送信され、そのネイバーを特定の(S,G)パスまたは(*,G)パスに追加または削除します。PIMマルチキャストパケットは、Time-To-Live(TTL)=1で送信されるリンクローカルマルチキャストパケットです。これらのパケットはすべて、既知のAll-PIM-Routersアドレスへのマルチキャストです。224.0.0.13.つまり、このような攻撃はすべて、攻撃を受けるルータと同じサブネット上で発生する必要があります。攻撃には、偽造Hello、Join/Prune、およびAssertパケットが含まれます。

> **注**：PIMマルチキャストパケットのTTL値を1より大きい値に人為的に増加または調整しても、問題は発生しません。All-PIM-Routersアドレスは常にルータでローカルに受信され、処理されます。通常の正規のルータによって直接転送されることはありません。

PIM-SMレジスタメッセージの潜在的なフラッディングからRPを保護するために、DRはこれらのメッセージをレート制限する必要があります。**ip pim register-rate-limit**コマンドを使用します。

```
ip pim register-rate-limit <count>
```

図 8:PIM-SMレジスタトンネル制御

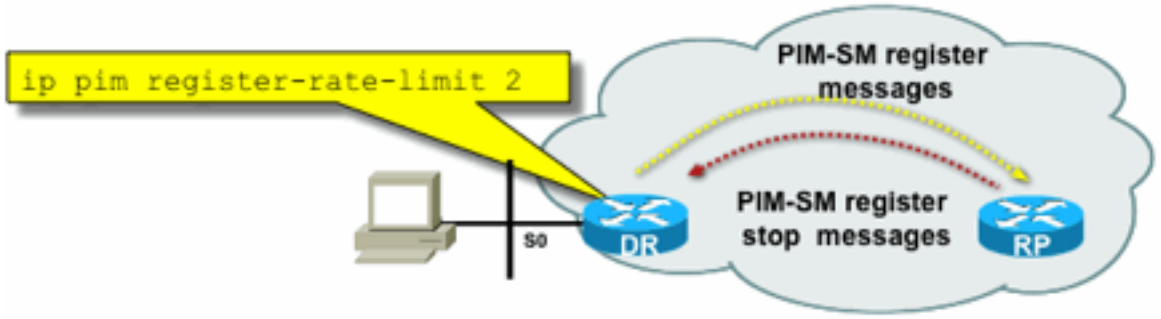

Fig8_PIMSM_Reg Tunnel

PIMユニキャストパケットを使用してRPを攻撃できます。そのため、RPはインフラストラクチャACLによってこのような攻撃から保護できます。マルチキャストの送信側と受信側はPIMパケットを送信する必要がないため、通常はPIMプロトコル（IPプロトコル103）をサブスクライバエッジでフィルタリングできます。

自動RP制御 – RPアナウンスフィルタ

ip pim rp-announce filterコマンドは、可能な場合にAuto-RPで設定できる追加のセキュリティ対策です。

```
ip pim rp-announce-filter
```

これは、どのルータがどのグループ範囲/グループモードの候補RPとして受け入れられるかを制御するためにMapping Agentで設定できます。

図 9:Auto-RP - RPアナウンスフィルタ

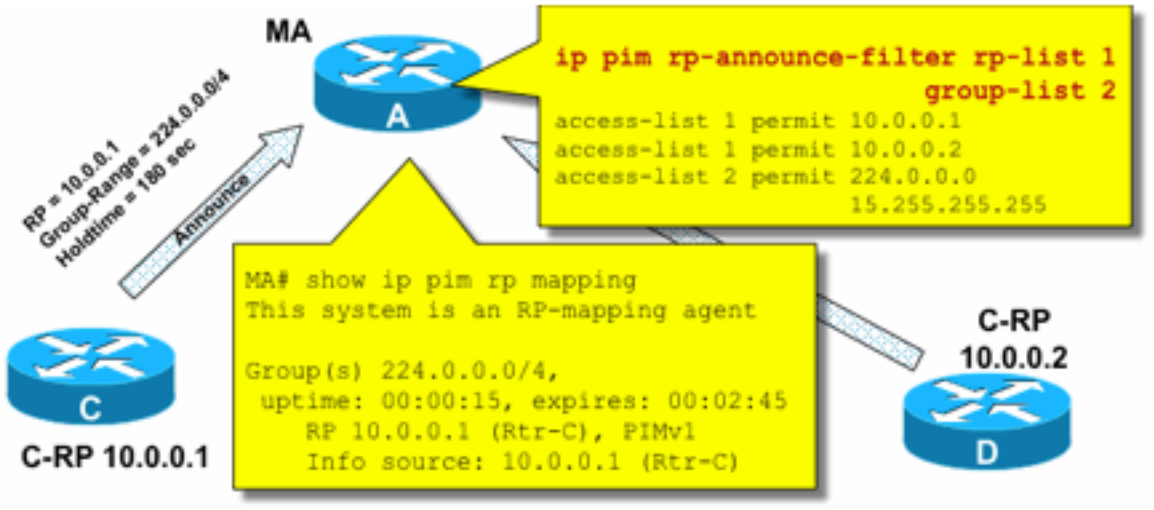

Fig9_AutoRP_RP_Announce

Auto-RP制御：Constrain Auto-RPメッセージ

multicast boundaryコマンドを使用して、AutoRPパケット、RP-announce(224.0.1.39)またはRP-discover(224.0.1.40)を特定のPIMドメインに制限します。

```
ip multicast boundary
```

図 10：マルチキャスト境界コマンド

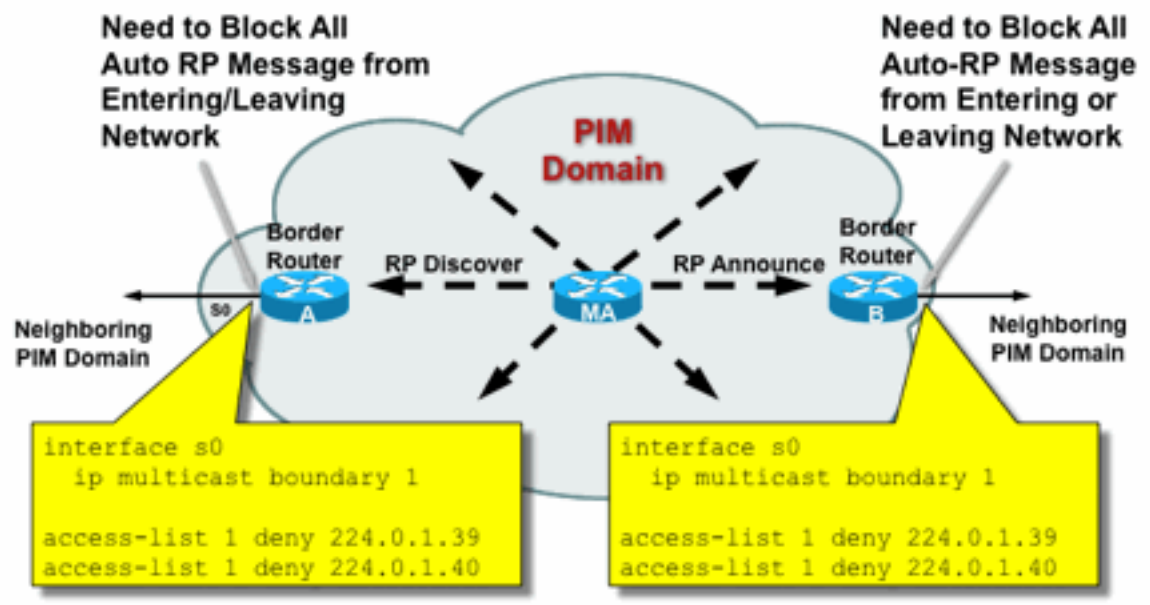

Fig10_Mcast_Boundary

BSR制御 – BSRメッセージの制約

ip pim bsr-border PIMドメインの境界でBSRメッセージをフィルタリングするコマンド。BSRメッセージはリンクローカルマルチキャストでホップバイホップ転送されるため、ACLは必要ありません。

図 11：BSRボーダー

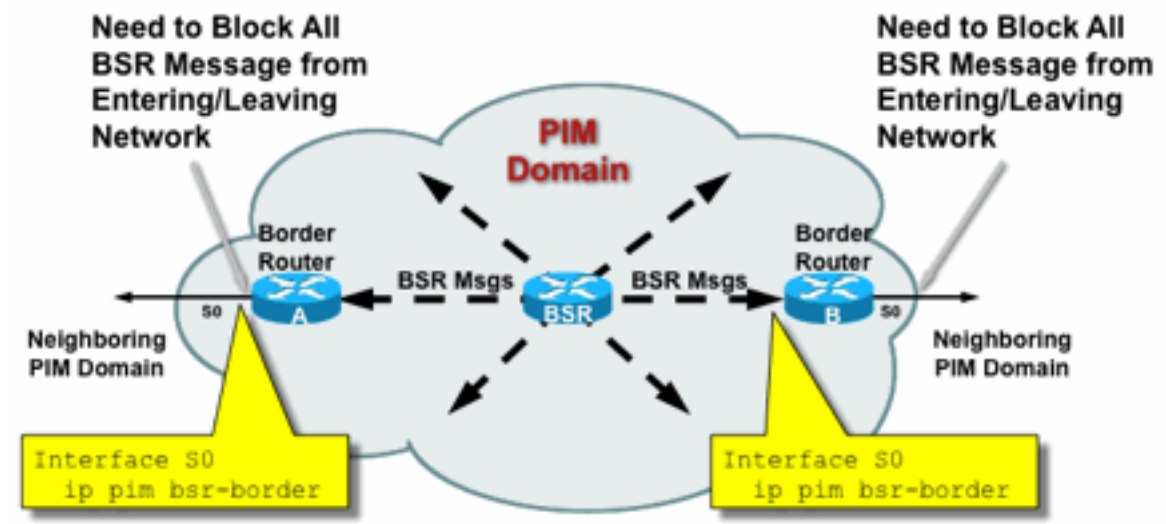

Fig11_BSR_Router

RP/PIM-SM関連フィルタ

この最後のセクションでは、PIM-SPおよびRPコントロールプレーンパケットに対するフィルタと、Auto-RP、BSR、およびMSDPメッセージについて説明します。

Auto-RPフィルタ

図12に、アドレススコープと組み合わせたAuto-RPフィルタの例を示します。領域をバインドする2つの方法を示します。2つのACLは、Auto-RPの観点からは同等です。

図 12：自動RPフィルタ/スコープ

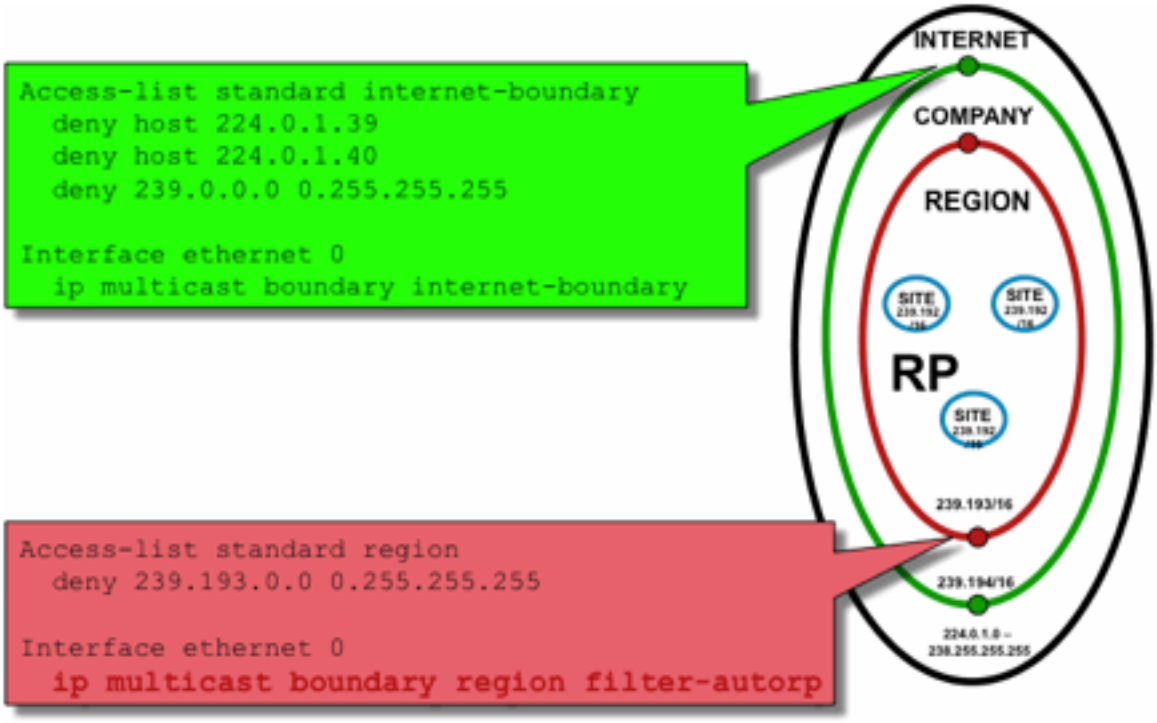

Fig12_AutoRP_Filtering_Scoping

Auto-RPのインターフェイス境界フィルタの概念は、Auto-RPアナウンスがサポートする地域にのみ届くようにすることです。地域、会社、およびインターネット全体のスコープが定義され、それぞれのスコープにはRPとAuto-RPアドバタイズメントがあります。管理者は、リージョナルRPがリージョナルルータに認識され、会社のRPがリージョナルルータと会社のルータに認識され、インターネットRPがグローバルに使用可能であるようにすることだけを望んでいます。スコープのレベルを上げることもできます。

図に示すように、Auto-RPパケットをフィルタリングする方法には、基本的に次の2種類があります。インターネット境界は、auto-rp制御グループ（224.0.1.39および224.0.1.40）を明示的に呼び出します。その結果、すべてのAuto-RPパケットに対してフィルタが適用されます。この方法は、Auto-RPパケットが通過しない管理ドメインのエッジで使用できます。Region boundaryは、filter-auto-rpキーワードを使用して、Auto-RPパケット内のrp-to-group-rangeアナウンスを調べます。アナウンスがACLによって明示的に拒否されると、パケットが転送される前にAuto-RPパケットから削除されます。この例では、エンタープライズ全体のRPがリージョン内で認識され、リージョン全体のRPはリージョンからエンタープライズの他の部分までの境界でフィルタリングされます。

ドメイン間フィルタとMSDP

この例では、ISP1はPIM-SM中継プロバイダーとして機能します。ネイバーとのMSDPピアリングのみをサポートし、境界ルータでは(S,G)トラフィックのみを受け入れ、(*,G)トラフィックは受け入れません。

ドメイン間（通常は自律システム間）では、次の2つの基本的なセキュリティ対策を講じる必要があります。

1. **multicast boundary**コマンドを使用して、データプレーンを保護します。これにより、マルチキャストトラフィックが定義されたグループ（および潜在的な送信元）に対してのみ受け入れられるようになります。
2. ドメイン間コントロールプレーントラフィック(MSDP)を保護します。 これは、次の複数のセキュリティ対策で構成されています。MSDPコンテンツ制御、状態制限、およびネイバー認証。

図13は、ISP1の境界ルータの1つでインターフェイスフィルタを設定する例を示しています。

multicast boundaryコマンドを使用して、「host 0.0.0.0」および管理スコープアドレスに対するフィルタによって、ドメイン境界インヒビット(*,G)結合でデータプレーンを保護するには、次の手順を実行します。

図 13：ドメイン間(*,G)フィルタ

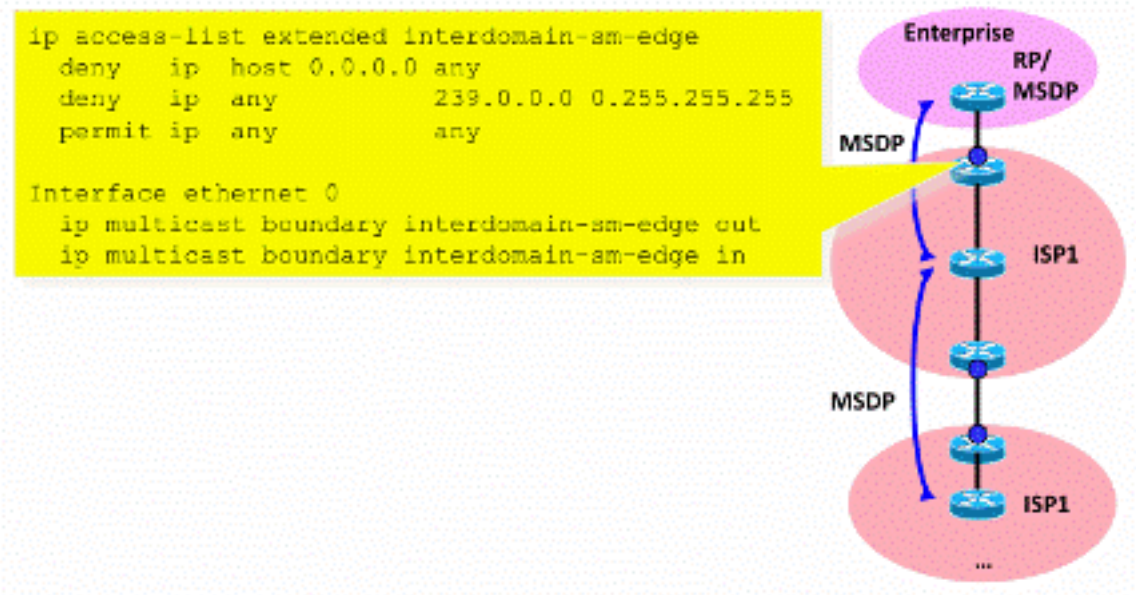

fig13_Interdomain_Filter

コントロールプレーンを保護するには、次の3つの基本的なセキュリティ対策によってMSDPを強化します。

1) MSDP SAフィルタ

これは、MSDP SAフィルタを介してMSDPメッセージの内容をフィルタリングする「ベストプラクティス」です。このフィルタの主な考え方は、インターネット全体のアプリケーションではな

く、送信元ドメインを越えて転送する必要のないアプリケーションおよびグループに対して、マルチキャスト状態の伝播を回避することです。理想的には、セキュリティの観点から、フィルタは既知のグループ（および潜在的な送信者）のみを許可し、未知の送信者やグループを拒否します。

通常、許可されたすべての送信者やグループを明示的にリストすることはできません。グループごとに1つのRPを持つPIM-SMドメインには、デフォルトの設定フィルタを使用することを推奨します（MSDPメッシュグループは使用しません）。

```
!--- Filter MSDP SA-messages.
         !--- Replicate the following two rules for every external MSDP peer.
         !
         ip msdp sa-filter in <peer_address> list 111
         ip msdp sa-filter out <peer_address> list 111
         !
         !--- The redistribution rule is independent of peers.
         !
         ip msdp redistribute list 111
         !
         !--- ACL to control SA-messages originated, forwarded.
         !
         !--- Domain-local applications.
         access-list 111 deny   ip any host 224.0.2.2     !
         access-list 111 deny   ip any host 224.0.1.3     ! Rwhod
         access-list 111 deny   ip any host 224.0.1.24    ! Microsoft-ds
         access-list 111 deny   ip any host 224.0.1.22    ! SVRLOC
         access-list 111 deny   ip any host 224.0.1.2     ! SGI-Dogfight
         access-list 111 deny   ip any host 224.0.1.35    ! SVRLOC-DA
         access-list 111 deny   ip any host 224.0.1.60    ! hp-device-disc
         !--- Auto-RP groups.
         access-list 111 deny   ip any host 224.0.1.39
         access-list 111 deny   ip any host 224.0.1.40
         !--- Scoped groups.
         access-list 111 deny   ip any 239.0.0.0 0.255.255.255
         !--- Loopback, private addresses (RFC 6761). access-list 111 deny ip 10.0.0.0
0.255.255.255 any access-list 111 deny ip 127.0.0.0 0.255.255.255 any access-list 111 deny ip
172.16.0.0 0.15.255.255 any access-list 111 deny ip 192.168.0.0 0.0.255.255 any !--- Default
SSM-range. Do not do MSDP in this range. access-list 111 deny ip any 232.0.0.0 0.255.255.255
access-list 111 permit ip any any !
```

できるだけ厳密にフィルタリングし、両方向でインバウンドとアウトバウンドを行うことを推奨します。

MSDP SAフィルタの推奨事項の詳細については、を参照してください。
https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) MSDP状態の制限

複数の自律システム(AS)間でMSDPを有効にする場合は、ネイバーから受信した「Source-Active」(SA)メッセージのために、ルータに構築されるステートの量を制限することをお勧めします。**ip msdp sa-limit**コマンドを使用できます。

```
ip msdp sa-limit <peer> <limit>
```

図 14：MSDPコントロールプレーン

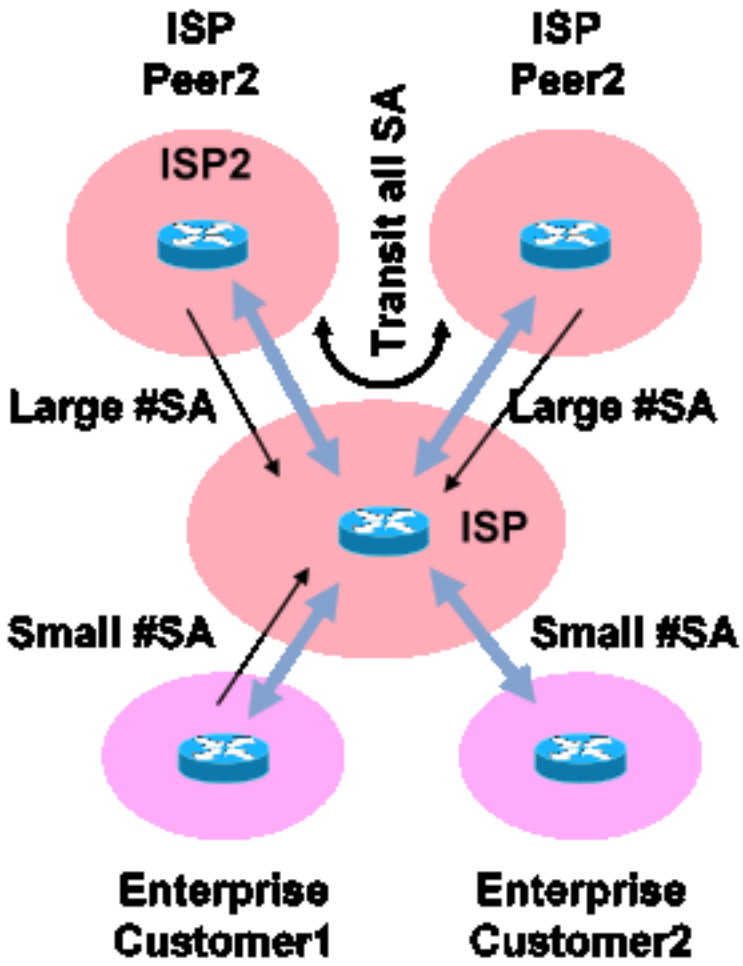

fig14_MSDP_ControlPlane

ip msdp sa-limitコマンドを使用すると、MSDPピアから受け入れられたSAメッセージによって作成されるSA状態の数を制限できます。簡単な経験則に基づく推奨事項には、次のようなものがあります。

- スタブネイバーからの小さい制限
- 中継ネイバーからの大きな制限(インターネット#SAsの最大制限など)
- トランジットISP：プラットフォームが#SAsポートできる最大値を設定する

3) MSDP MD5ネイバー認証

MSDPピアでMessage-Digest Algorithm(MD5)パスワード認証を使用することを推奨します。これは、RFC 6691で説明されているBGPの保護に相当するTCP MD5シグニチャオプションを使用します。

図 15：MSDP MD5ネイバー認証

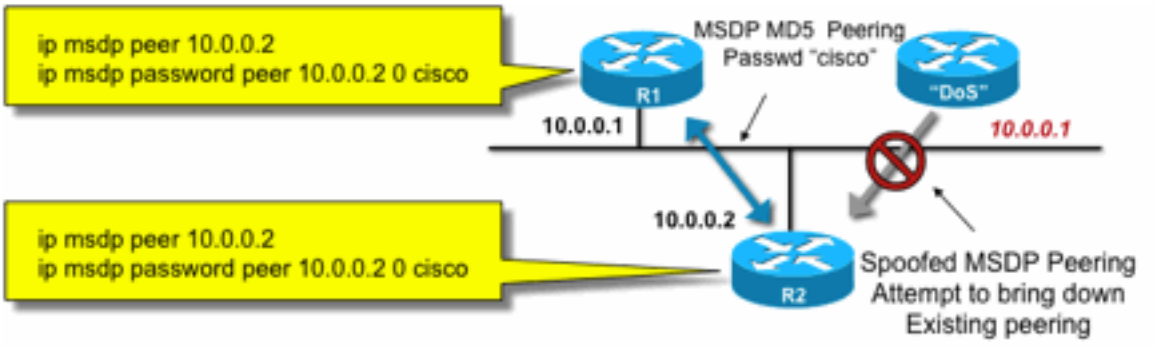

Fig15_MSDP_MD5Auth

次の3つのMSDPセキュリティの推奨事項は、異なる目標を追求します。

- ネイバー認証（MD5を使用）により、信頼できるMSDPピアだけがメッセージを送信できるようになります。
- SAフィルタにより、信頼できるMSDPピアでも、事前に合意された送信元/グループポリシーに従ったSAアナウンスだけを送信できます。
- SA制限により、正当なピアからの正当な(S,G)アナウンスがあっても、使用可能なメモリを使い果たすことができなくなります。

送信者/送信元の問題

送信側に起因するマルチキャストセキュリティの問題の多くは、適切なユニキャストセキュリティメカニズムで軽減できます。推奨されるベストプラクティスは、次のユニキャストセキュリティメカニズムです。

- **送信元アドレスのスプーフ**保護（アクセスレイヤ用のユニキャストリバースパス転送、uRPFまたはACL、およびIPソースガード）
- **インフラス**トラクチャACL(deny ip any (to) <core address space>)

このような対策は、コアへの標的型攻撃をブロックするために使用できます。これにより、たとえば、RPへのPIMユニキャストパケットを使用する攻撃などの問題も解決できます。RPはネットワークの「内部」であり、インフラストラクチャACLによって保護されます。

パケットフィルタベースのアクセス制御：コントロールソース

図16の例では、フィルタはファーストホップマルチキャストルータ（代表ルータ）のLANインターフェイス(E0)に設定されています。 フィルタは、「source」という拡張アクセスコントロールリスト(ACL)によって定義されます。このACLは、ソースLANに接続された代表ルータのソース側インターフェイスに適用されます。実際には、マルチキャストトラフィックの性質により、送信元がアクティブになる可能性のあるすべてのLAN側インターフェイスで同様のフィルタを設定する必要があります。ソースアクティビティが発生する場所を正確に知ることはできないため、このようなフィルタをネットワーク内のすべての入力ポイントに適用することをお勧めします。

図 16：コントロールソース

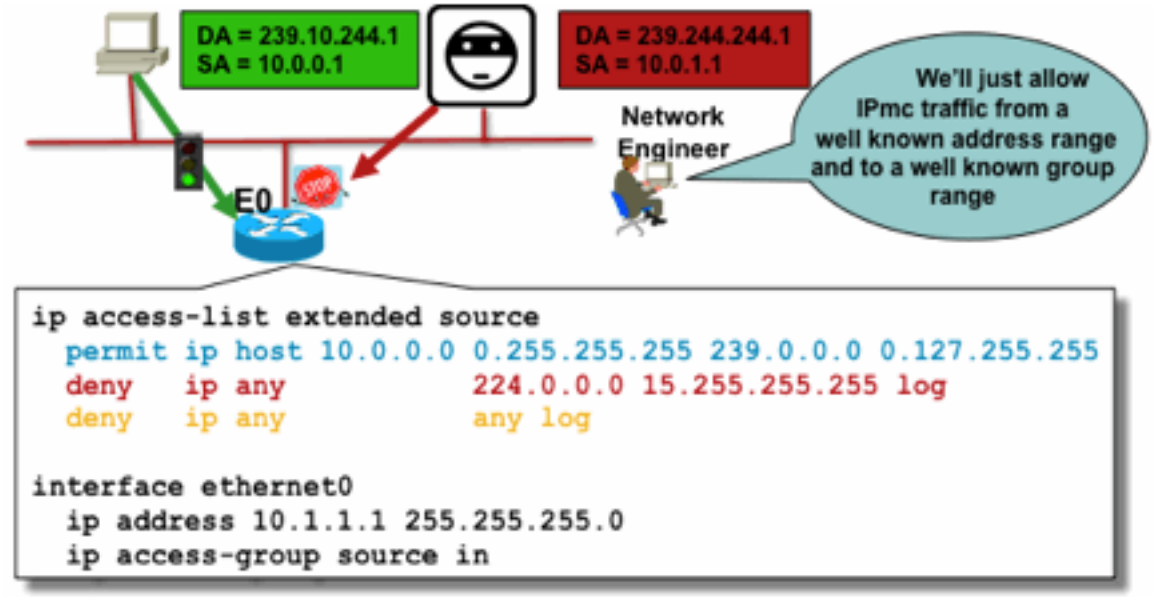

Fig16_Controlling_Sources

このフィルタの目的は、特定の送信元アドレスまたは送信元アドレスの範囲から特定のグループまたはグループアドレスの範囲へのトラフィックを防止することです。このフィルタは、PIMがmrouteを作成する前に機能し、ステートの制限に役立ちます。

これは標準データプレーンACLです。これはハイエンドプラットフォームのASICに実装され、パフォーマンスの低下は発生しません。データプレーンACLは、不要なトラフィックによるコントロールプレーンへの影響を最小限に抑えるため、直接接続された送信元に対してはコントロールプレーンよりも推奨されます。また、パケットの送信先となる宛先（IPマルチキャストグループアドレス）を制限することも非常に効果的です。これはルータコマンドであるため、スプーフィングされた送信元IPアドレスを克服することはできません（このセクションの前半を参照）。したがって、追加のレイヤ2(L2)メカニズムを提供するか、特定のローカルエリアネットワーク/仮想ローカルエリアネットワーク(LAN/VLAN)に接続できるすべてのデバイスに対して一貫したポリシーを提供することを推奨します。

> **注**：ACLの「log」キーワードは、特定のACLエントリに対するヒットを理解するのに非常に便利です。ただし、これはCPUリソースを消費するため、慎重に処理する必要があります。また、ハードウェアベースのプラットフォームでは、ACLログメッセージはCPUによって生成されるため、CPUへの影響を考慮する必要があります。

PIM-SMソース制御

セキュリティの観点から見たASM/PIM-SMアーキテクチャの実際の利点の1つは、ランデブーポイントがネットワーク内のすべてのソースに対して任意のグループ範囲の単一の制御ポイントを提供するということです。これは、accept-registerフィルタと呼ばれるデバイスで利用できます。このフィルタのコマンドは次のとおりです。

```
ip pim accept-register / ipv6 pim accept-register
```

図 17：PIM-SMソース制御

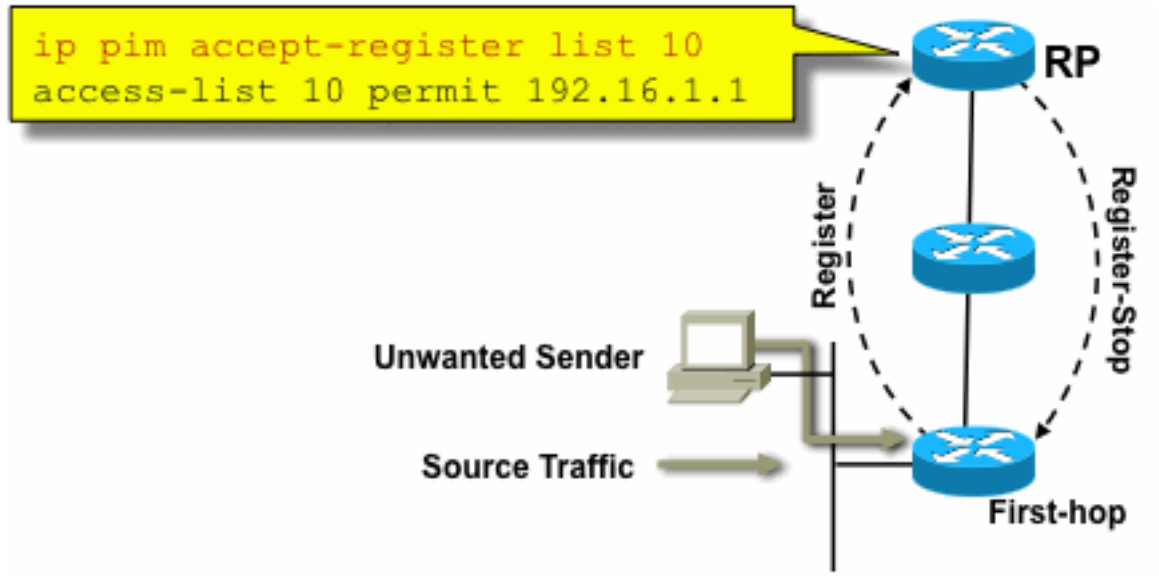

Fig17_PIMSM_Control

PIM-SMネットワークでは、このコマンドを使用して不要なトラフィックソースを制御できます。送信元トラフィックがファーストホップルータに到達すると、ファーストホップルータ(DR)が(S,G)状態を作成し、PIMソースレジスタメッセージをRPに送信します。送信元がaccept-registerフィルタリスト（RPで設定）にリストされていない場合、RPはRegisterを拒否し、即時Register-StopメッセージをDRに返します。

この例では、送信元アドレスだけをフィルタリングする単純なACLがRPに適用されています。RPで拡張ACLを使用して、送信元とグループをフィルタリングすることもできます。

RPで**pim accept-register**コマンドを使用すると、発信元のファーストホップルータでPIM-SM(S,G)状態が引き続き作成されるため、発信元フィルタには欠点があります。その結果、送信元に対してローカルで、送信元とRPの間にある受信側でトラフィックが発生する可能性があります。さらに、**pim accept-register**コマンドはRPのコントロールプレーンで動作します。これは、偽のレジスタメッセージでRPをオーバーロードするために使用され、DoS状態を引き起こす可能性があります。

pim accept-registerコマンドは、ネットワークに入ってくるすべての入力ポイントに対して、すべてのDRに単純なデータプレーンACLを適用するなどの他の方法に加えて、RPに適用することを推奨します。DRの入力ACLは、完全に設定され運用されているネットワークでは十分ですが、エッジルータで設定が誤っている場合のセカンダリセキュリティメカニズムとして**pim accept-register**コマンドををRPに設定することを推奨します。同じ目標を持つ階層化されたセキュリティメカニズムは「多層防御」と呼ばれ、セキュリティの一般的な設計原則です。

レシーバの問題：コントロールIGMP/MLD

ほとんどのレシーバの問題は、IGMP/MLDレシーバプロトコルインタラクションの領域に分類されます。

図 18：制御IGMP

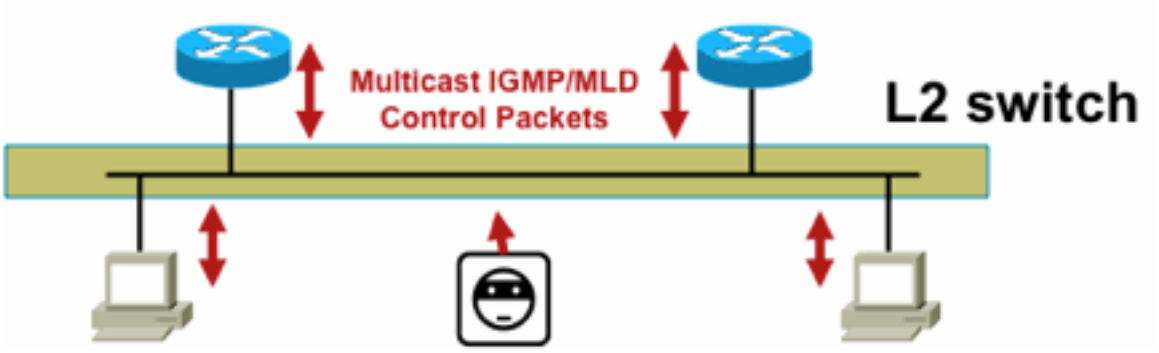

fig18_Controlling_IGMP

IGMPまたはMLDパケットがフィルタリングされる場合は、次の点に注意してください。

- IPv4:IGMPはIPv4プロトコルタイプ（IPv4プロトコル2）です
- IPv6：MLDは、ICMPv6プロトコルタイプのパケットで伝送されます

IGMPプロセスは、IPマルチキャストが有効になるとすぐに、デフォルトで有効になります。IGMPパケットは次のプロトコルも伝送するため、マルチキャストが有効になっている場合は常に、次のプロトコルがすべて有効になります。

- PIMv1:PIMv1はPIMの最初のバージョンであり、移行のためにCisco IOSでは常に有効になっています。現在の導入では、すべてPIMv2を使用します。
- Mrinfo:Mrinfoは、マルチキャストネイバーを表示するためにCisco IOSが継承したUnixコマンドです。Ciscoでは、mrinfoコマンドの代わりにSNMPを使用することを推奨しています。
- DVMRP:DVMRPは、スケーリング特性が非常に限られているレガシーなデンスモードのディスタンスベクタープロトコルです。DVMRPに対するCisco IOSサポートは廃止されたか、すでに廃止されています。
- Mtrace - Mtraceはユニキャスト「traceroute」に相当するマルチキャストであり、便利なツールです

詳細については、「IANAのインターネットグループ管理プロトコル(IGMP)タイプ番号」を参照してください。

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254

Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
 0  172.16.0.10
-1  172.16.0.8 PIM  thresh^ 0  0 ms
-2  172.16.0.6 PIM  thresh^ 0  2 ms
-3  172.16.0.5 PIM  thresh^ 0  894 ms
-4  172.16.0.3 PIM  thresh^ 0  893 ms
-5  172.16.0.2 PIM  thresh^ 0  894 ms
-6  172.16.0.1 PIM  thresh^ 0  893 ms
```

ユニキャストIGMPパケット（IGMP/UDLR用）は、攻撃パケットである可能性が高く、有効なIGMPプロトコルパケットではないため、フィルタリングできます。ユニキャストIGMPパケットは、単方向リンクおよびその他の例外条件をサポートするために、Cisco IOSでサポートされています。

偽造されたIGMP/MLDクエリーパケットは、予想よりも低いIGMPバージョンになる可能性があります。

特に、低いIGMPバージョンで送信されたクエリによって、このクエリを受信したすべてのホストが低いバージョンに戻される可能性があるため、ホストはIGMPクエリを送信しないことが理想的です。IGMPv3/SSMホストが存在する場合、SSMストリームを「攻撃」できます。IGMPv2の場合、これは長いリーブレーテンシーを引き起こす可能性があります。

単一のIGMPクエリアを持つ非冗長LANが存在する場合、ルータは受信したIGMPクエリーをドロップする必要があります。

冗長または共通のパッシブLANが存在する場合は、IGMPスヌーピング対応のスイッチが必要です。この場合に役立つ2つの機能があります。

- ルータガード
- IGMP Minimum Versionコマンド

ルータガード

スイッチがそのポートでマルチキャストルータコントロールパケット（IGMP一般クエリー、PIM Hello、またはCGMP Hello）を受信すると、すべてのスイッチポートがマルチキャストルータポートになる可能性があります。スイッチポートがマルチキャストルータポートになると、すべてのマルチキャストトラフィックがそのポートに送信されます。これは「ルータガード」で防ぐことができます。Router Guard機能では、IGMPスヌーピングを有効にする必要はありません。

ルータガード機能を使用すると、指定したポートをマルチキャストホストポートに指定できます。マルチキャストルータ制御パケットを受信しても、ポートはルータポートになることはできません。

これらのパケットタイプは、Router Guardが有効になっているポートで受信されると廃棄されます。

- IGMPクエリメッセージ
- IPv4 PIMv2メッセージ
- IGMP PIMメッセージ(PIMv1)
- IGMP DVMRPメッセージ
- ルータポートグループ管理プロトコル(RGMP)メッセージ
- Cisco Group Management Protocol(CGMP)メッセージ

これらのパケットが廃棄されると、ルータガードによってパケットが廃棄されたことを示す統計情報が更新されます。

IGMP最小バージョン

許可されるIGMPホストの最小バージョンを設定できます。たとえば、すべてのIGMPv1ホスト、またはすべてのIGMPv1およびIGMPv2ホストを拒否できます。このフィルタは、メンバーシップレポートにのみ適用されます。

ホストが共通の「パッシブ」LAN（たとえば、IGMPスヌーピングをサポートしていないスイッチやIGMPスヌーピング用に設定されていないスイッチ）に接続されている場合は、そのような誤ったクエリーに対してルータが実行できることはありません。その場合にトリガーされる「旧バージョン」メンバーシップレポートを無視し、自分自身をフォールバックしないことが唯一の条件です。

IGMPクエリはすべてのホストから認識できる必要があるため、「有効なルータ」からのIGMPクエリを認証するために、静的キーIPSecなどの事前共有キーを使用してHash-based message authentication(HMAC)メカニズムを使用することはできません。2台以上のルータが共通のLANセ

グメントに接続されている場合は、IGMPクエリアの選択が必要です。この場合、使用できるフィルタは、クエリーを送信する他のIGMPルータの送信元IPアドレスに基づくip access-groupフィルタだけです。

「通常の」マルチキャストIGMPパケットを許可する必要があります。

このフィルタをレシーバポートで使用すると、「正常な」IGMPパケットだけを許可し、既知の「不良」パケットをフィルタリングできます。

```
ip access-list extended igmp-control
   <snip>
   deny   igmp any any  pim        ! No PIMv1
   deny   igmp any any  dvmrp      ! No DVMRP packets
   deny   igmp any any  host-query ! Do not use this command with redundant routers.
                                   ! In that case this packet type is required !
   permit igmp any host 224.0.0.22 ! IGMPv3 membership reports
   permit igmp any any  14         ! Mtrace responses
   permit igmp any any  15         ! Mtrace queries
   permit igmp any 224.0.0.0 10.255.255.255 host-query  ! IGMPv1/v2/v3 queries
   permit igmp any 224.0.0.0 10.255.255.255 host-report ! IGMPv1/v2 reports
   permit igmp any 224.0.0.0 10.255.255.255 7           ! IGMPv2 leave messages
   deny   igmp any any             ! Implicitly deny unicast IGMP here!
<snip> permit ip any any ! Permit other packets interface ethernet 0 ip access-group igmp-
control in
```

注：このタイプのIGMPフィルタは、受信ACLまたはCoPPで使用できます。どちらのアプリケーションでも、ルーティングや管理プレーンプロトコルなど、処理される他のトラフィックのフィルタと組み合わせる必要があります。

図 19：ホスト受信側のアクセスコントロール

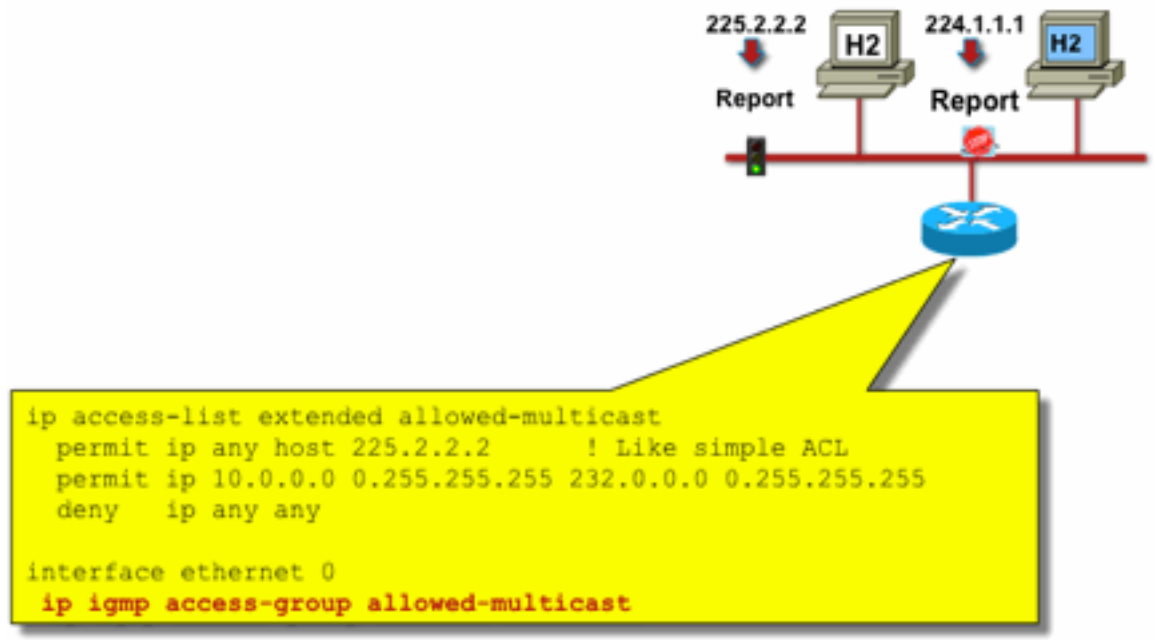

Fig19_Host_Receiver_Access

受信側へのトラフィックをフィルタリングするには、データプレーントラフィックではなく、コントロールプレーンプロトコルIGMPをフィルタリングします。IGMPはマルチキャストトラフィ

ックを受信するために必要な前提条件であるため、データプレーンフィルタは必要ありません。

特に、どのマルチキャストフローの受信者が参加できるか（コマンドが設定されているインターフェイスに接続されるか）を制限できます。 この場合は、**ip igmp access-group / ipv6 mld access-group** コマンドを使用します。

ip igmp access-group / ipv6 mld access-group
ASMグループの場合、このコマンドは宛先アドレスに基づいてフィルタリングするだけです。ACLの送信元IPアドレスは無視されます。IGMPv3/MLDv2を使用するSSMグループでは、送信元と宛先のIPがフィルタリングされます。

次の例では、すべてのIGMPスピーカに対して特定のグループをフィルタリングします。

```
access-list 1 deny 226.1.0.0 0.0.255.255
access-list 1 permit any log
! interface ethernet 1/3 ip igmp access-group 1
```

次の例では、特定のグループの特定のIGMPスピーカ（つまり、特定のマルチキャスト受信側）をフィルタリングします。

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface Ethernet0/3
 ip igmp access-group test5
```

注：ASMグループでは、ソースは無視されることに注意してください。

アドミッション制御

アクセス制御は、ネットワークの状態に関係なく、特定のフローに対してバイナリ、yesまたはnoのいずれかの応答を提供します。対比によるアドミッション制御では、送信者/受信者が使用できるリソースの数を制限します。これは、送信者/受信者がアクセス制御メカニズムを通過したと仮定します。マルチキャスト環境でのアドミッション制御に役立つさまざまなデバイスが用意されています。

グローバルおよびインターフェイスごとのIGMP制限

対象となるマルチキャスト受信側に最も近いルータでは、グローバルおよびインターフェイスごとに参加するIGMPグループの数を制限できます。**ip igmp limit/ipv6 mld limit**コマンドを使用できます。

ip igmp limit <n> [except <ext-acl>]
ipv6 mld limit <n> [except <ext-acl>]
この制限は、常にインターフェイスごとに設定し、グローバルに設定することをお勧めします。いずれの場合も、この制限はIGMPキャッシュ内のエントリの数を示します。

次の2つの例は、このコマンドを使用して、家庭用ブロードバンドネットワークのエッジでグルー

プ数を制限する方法を示しています。

例1：受信したグループをSDRアナウンスと1つの受信チャネルだけに制限する

セッションディレクトリ(SDR)は、一部のマルチキャスト受信者に対するチャネルガイドとして機能します。詳細については、RFC 2327を参照してください。

一般的な要件は、SDグループと1つのチャネルを受信するようにレシーバを制限することです。次の設定例を使用できます。

```
ip access-list extended channel-guides
  permit ip any host 239.255.255.254 ! SDR announcements
  deny   ip any any

ip igmp limit 1 except channel-guides

interface ethernet 0
  ip igmp limit 2 except channel-guides
```

この例のアクセスリストでは、チャネルガイドのみを指定しています。グローバル**ip igmp limit**コマンドは、各IGMPソースを1つのチャネル(1)に制限しますが、チャネルガイドは含まれません。チャネルガイドは常に受信できます。interfaceコマンドはグローバルコマンドを上書きし、このインターフェイスでチャネルガイドに加えて2つのチャネルを受信できるようにします。

例2：集約DSLAMリンクのアドミッション制御

このコマンドは、帯域幅アドミッション制御の形式を提供するためにも使用できます。たとえば、300のSDTVチャネル（それぞれ4 Mbps）を配信する必要があり、Digital-Subscriber-Line-Access-Multiplexer(DSLAM)への1 Gbpsリンクがある場合、ポリシーを決定してTV帯域幅を500 Mbpsに制限し、残りはインターネットなどの用途に使用することができます。この場合、IGMPの状態を500 Mbps/4 Mbps = 125 IGMP状態に制限できます。

この場合、次の設定を使用できます。

図 20：インターフェイスごとのIGMP制限の使用Agg-DSLAMリンクのアドミッション制御

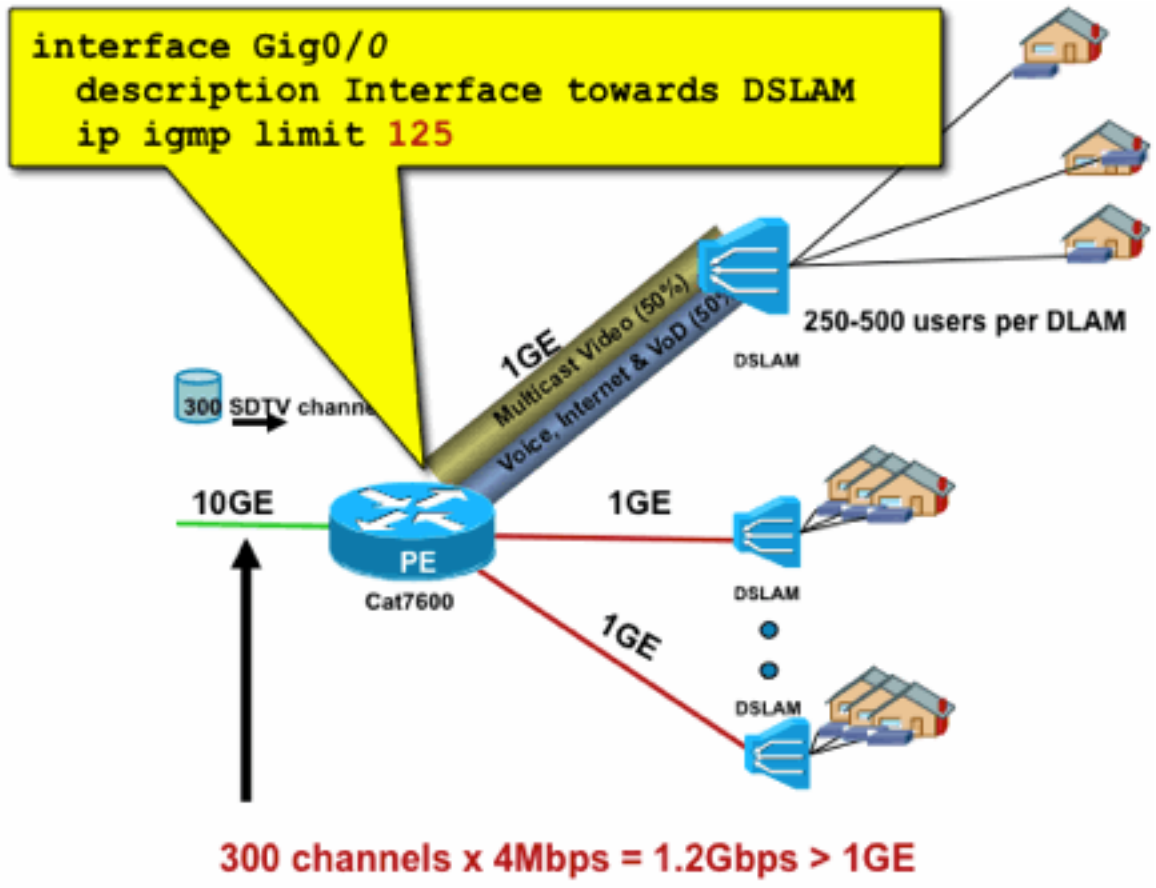

Fig20_PerInterface_IGMP

インターフェイスごとのmroute制限

インターフェイスごとのmroute状態制限の有効化は、より一般的な形のアドミッション制御です。発信インターフェイスのIGMPおよびPIM状態を制限するだけでなく、着信インターフェイスの状態制限の方法も提供します。

ip multicast limitコマンドを使用します。

ip multicast limit [rpf | out | connected] <ext-acl> <max>

状態は入出力インターフェイスで個別に制限できます。直接接続されたソースの状態は、「connected」キーワードを使用して制限することもできます。このコマンドの使用例を次に示します。

例1:Agg-DSLAMリンクの出力アドミッション制御

この例では、300のSD TVチャネルがあります。各SDチャネルが4 Mbpsを必要とし、合計が500 Mbps以下であると仮定します。最後に、Basic、Extended、およびPremiumバンドルのサポートが必要であると仮定します。帯域幅割り当ての例：

- 60 %/300 Mbps Basic
- 20 %/100 Mbps拡張
- 20 %/100 Mbps Premium

次に、チャネルごとに4 Mbpsを使用し、DSLAMアップリンクを次のように制限します。

- 基本75状態
- 拡張25状態
- プレミアム25州

PEAggからDSLAMに向かう発信インターフェイスに制限を設定します。

図 21：インターフェイスごとのmroute制限の使用Agg-DSLAMリンクのアドミッション制御

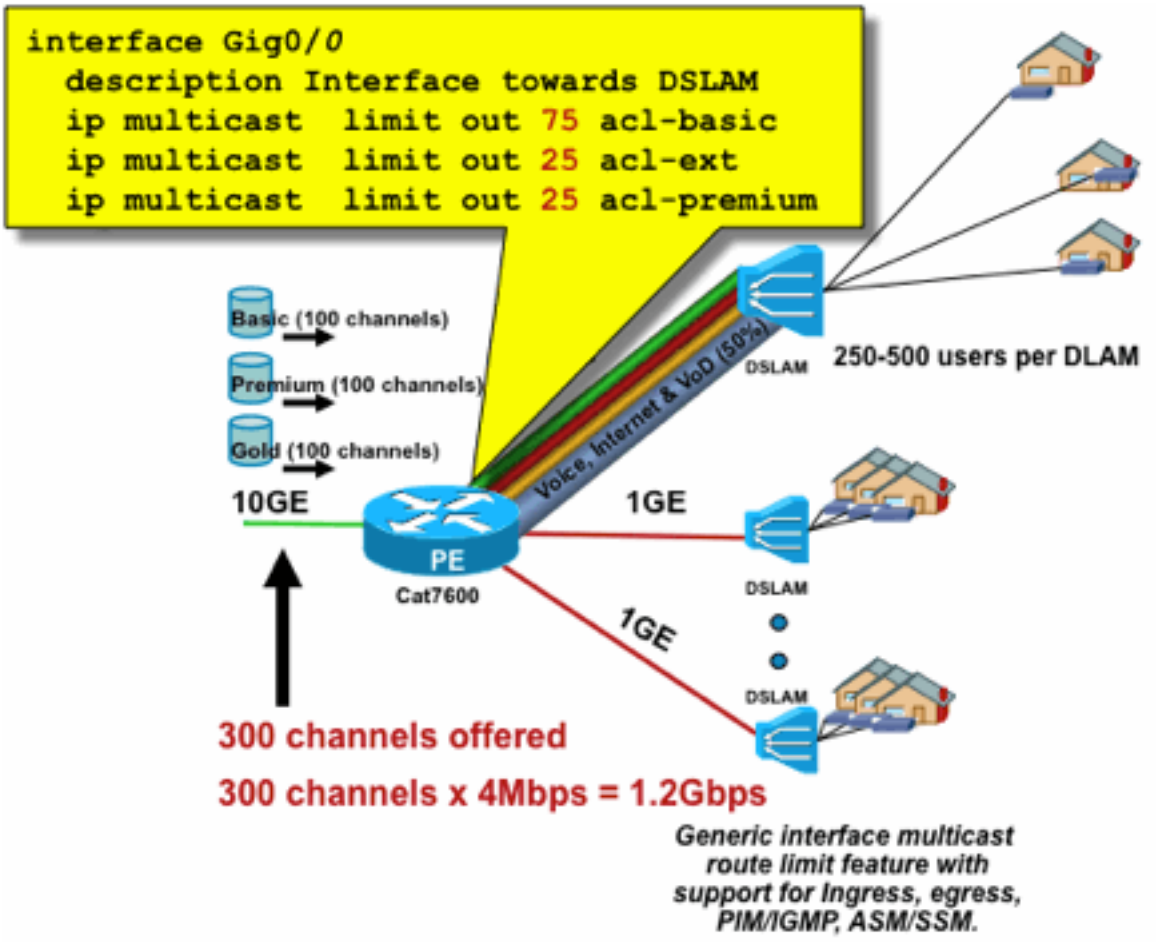

Fig21_PerInterface_Mroute

例2:Agg-DSLAMリンクの入力アドミッション制御

アップストリームデバイスの発信インターフェイスの「out」制限の代わりに、ダウンストリームデバイスのRPFインターフェイスでRPF制限を使用できます。これは実質的には前の例と同じ結果であり、ダウンストリームデバイスがCisco IOSデバイスでない場合に役立ちます。

図 22：インターフェイスごとのmroute制限の使用入力アドミッション制御

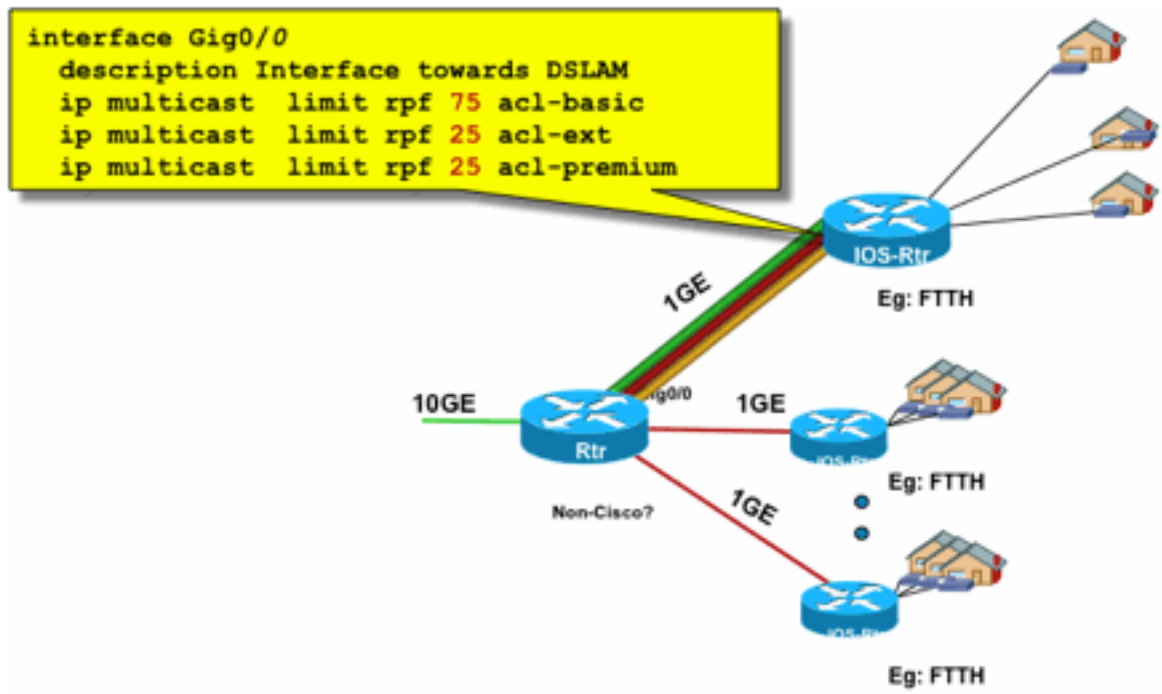

fig22_PerInt

erface_Mroute_inputControl

例3：帯域幅ベースの制限

複数のコンテンツプロバイダー間のアクセス帯域幅をさらに細分化し、各コンテンツプロバイダーにDSLAMへのアップリンクの帯域幅の公平な配分を提供できます。その場合は、**ip multicast limit cost**コマンドを使用します。

ip multicast limit cost <ext-acl> <multiplier>
このコマンドを使用すると、ipマルチキャスト制限の拡張ACLに一致する任意の状態に「コスト」（「強度」で指定した値を使用）を関連付けることができます。

このコマンドはグローバルコマンドであり、複数の同時コストを設定できます。

この例では、ネットワークへの各プロバイダーへの公平なアクセスを持つ3つの異なるコンテンツプロバイダーをサポートする必要があります。さらに、この例では、さまざまなタイプのMoving Picture Experts Group(MPEG)ストリームをサポートする必要があります。

MPEG2 SDTV:4 Mbps
MPEG2 HDTV:18 Mbps
MPEG4 SDTV:1.6 Mbps
MPEG4 HDTV:6 Mbps

このような場合、次の設定を使用して、各ストリームタイプに帯域幅コストを割り当て、残りの750 Mbpsを3つのコンテンツプロバイダー間で共有できます。

```
ip multicast limit cost acl-MP2SD-channels   4000 ! from any provider ip multicast limit cost
acl-MP2HD-channels 18000 ! from any provider ip multicast limit cost acl-MP4SD-channels 1600 !
from any provider ip multicast limit cost acl-MP4HD-channels 6000 ! from any provider !
interface Gig0/0 description --- Interface towards DSLAM --- <snip> ! CAC ip multicast limit out
250000 acl-CP1-channels ip multicast limit out 250000 acl-CP2-channels ip multicast limit out
```

```
250000 acl-CP3-channels
```

図 23：インターフェイスごとのmroute状態制限のコスト係数

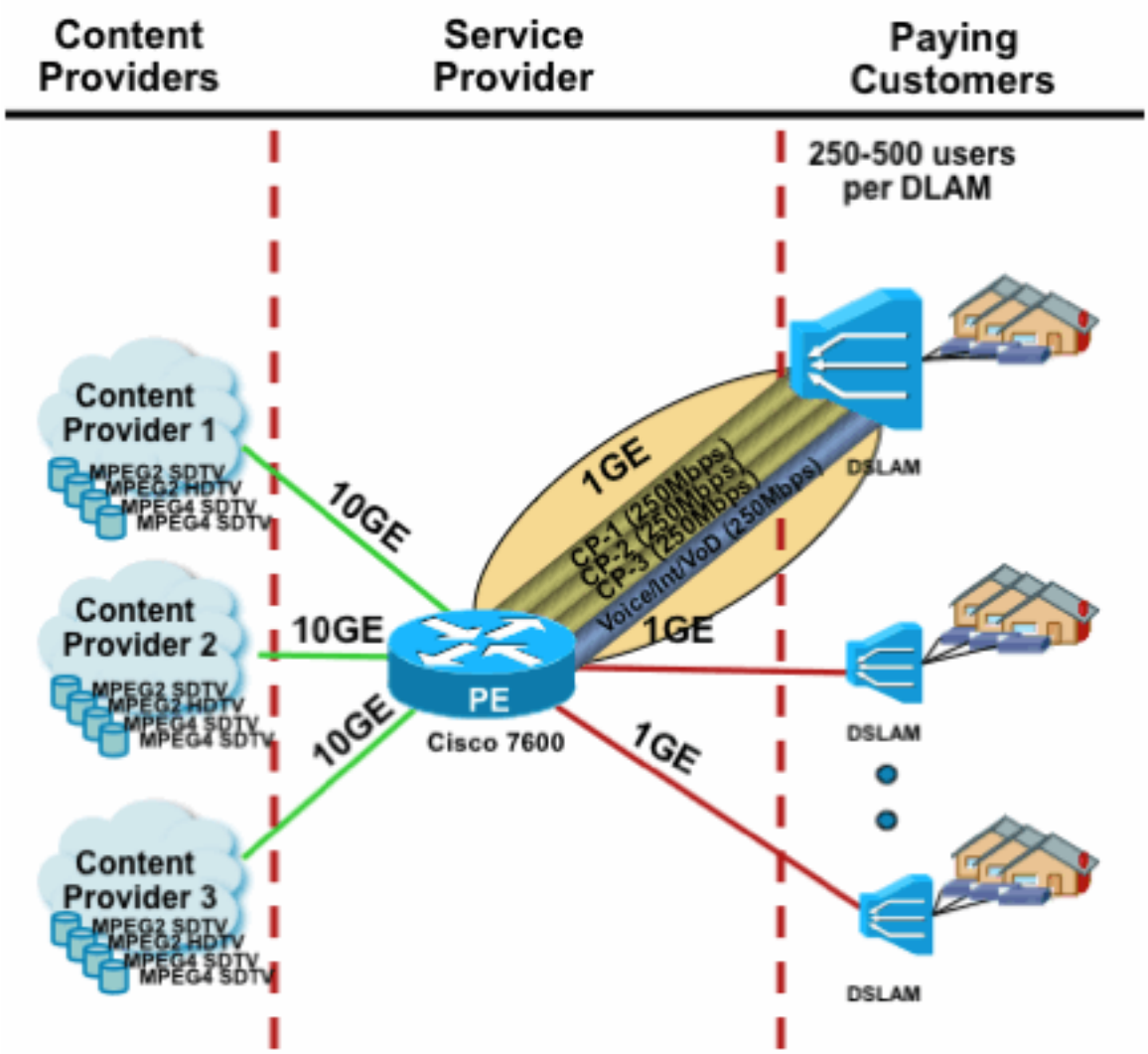

Fig23_Cost_P

erInterface

マルチキャストとIPSec

GET VPNの概要

ユニキャストと同様に、マルチキャストトラフィックも、機密性または整合性を保護するために保護する必要があります。このようなサービスが必要になる可能性のある主な領域は2つあります。

- マルチキャストストリームの暗号化（たとえば、マルチキャストを使用する多数の受信者に機密データをストリーミングするバンキングアプリケーションなど）：これはデータプレーンセキュリティです。
- マルチキャスト、OSPF、またはPIMを使用するコントロールプレーンプロトコルの暗号化。これはコントロールプレーンセキュリティです。

プロトコルとしてのIPSec(RFC 6040、7619、4302、4303、5282)は、ユニキャストトラフィック（RFCによる）に限定されています。 そこで、「セキュリティアソシエーション」(SA)が2つ

のユニキャストピア間で確立されます。IPSecをマルチキャストトラフィックに適用するには、GREトンネル内でマルチキャストトラフィックをカプセル化してから、IPSecをユニキャストであるGREトンネルに適用する方法があります。新しいアプローチでは、グループのすべてのメンバー間で確立された単一のセキュリティアソシエーションを使用します。これを実現する方法は、Group Domain of Interpretation(GDOI)(RFC 6407)で定義されています。

GDOIに基づいて、シスコはGroup Encryption Transport(GET)VPNというテクノロジーを開発しました。このテクノロジーは、「draft-ietf-msec-ipsec-extensions」で定義されている「アドレス保存を使用したトンネルモード」を使用します。GET VPNでは、最初にグループのすべてのメンバー間でグループセキュリティアソシエーションが確立されます。その後、トラフィックはESP（カプセル化されたセキュリティペイロード）またはAH（認証ヘッダー）のいずれかで保護されます。AHは、アドレス保存を伴うトンネルモードを使用します。

要約すると、GET VPNは、元のヘッダーのアドレス情報を使用するマルチキャストパケットをカプセル化し、グループポリシーに関連して内部パケットをESPなどで保護します。

GET VPNの利点は、マルチキャストトラフィックがセキュリティカプセル化メカニズムの影響を受けないことです。ルーテッドIPヘッダーアドレスは、元のIPヘッダーと同じままです。マルチキャストトラフィックは、GET VPNを使用する場合と使用しない場合で同じ方法で保護できます。

GET VPNノードに適用されるポリシーは、Group Key Serverで一元的に定義され、すべてのグループノードに配布されます。したがって、すべてのグループノードは同じポリシーを持ち、同じセキュリティ設定がグループトラフィックに適用されます。標準のIPSecと同様に、暗号化ポリシーは、保護する必要があるトラフィックのタイプを定義します。これにより、GET VPNをさまざまな目的で使用できます。

GET VPNを使用したマルチキャストデータプレーントラフィックの暗号化

ネットワーク全体の暗号化ポリシーがグループキーサーバに設定され、GET VPNエンドポイントに配布されます。このポリシーには、IPSecポリシー（IPSecモード）が含まれています。次に例を示します。トンネルモード（ヘッダーを保持している場合）、および使用するセキュリティアルゴリズム（AESなど）。 また、ACLで定義されているように、セキュリティで保護できるトラフィックを記述するポリシーも含まれています。

GET VPNは、マルチキャストおよびユニキャストトラフィックに使用できます。ユニキャストトラフィックを保護するポリシーは、ACLで定義できます。

```
permit ip 10.0.0.0   0.255.255.255   10.0.0.0   0.255.255.255
```

これにより、送信元IPが10/8で宛先IPが10/8であるすべてのトラフィックが暗号化されます。10/8から別のアドレスへのトラフィックなど、他のすべてのトラフィックはGET VPNによって無視されます。

マルチキャストトラフィックに対するGET VPNの適用は、技術的には同じです。たとえば、次のアクセスコントロールエントリ(ACE)を使用して、任意の送信元から各マルチキャストグループへのトラフィックを保護できます。

```
permit ip any 239.192.0.0 0.0.255.255
```

このポリシーは、すべての送信元(「any」)と、239.192で始まるすべてのマルチキャストグルー

プに一致します。他のマルチキャストグループへのトラフィックは保護されません。

> **注**：クリプトACLの構築には大きな注意が必要です。管理トラフィック、またはGET VPNドメインの外部から発信され、内部で終端するトラフィック（つまり、1つの暗号化エンドポイントのみを通過するトラフィック）は、GDOIポリシーから除外する必要があります。

よくある間違いは次のとおりです。

- permit ip any 224.0.0.0 0.255.255.255:また、たとえばピアルータ宛てのOSPFトラフィックやその他のコントロールプレーントラフィックも暗号化されます。
- 管理トラフィックは、ネットワーク内で終端する暗号化ポリシーから除外されません。これには、GDOIトラフィック自体も含まれます。

GET VPNを使用したコントロールプレーントラフィックの認証

一般に、信頼できるピアからメッセージが送信されるようにするため、ルーティングプロトコルなどのコントロールプレーントラフィックを認証することがベストプラクティスです。これは、BGPなどのユニキャストを使用するコントロールプレーンプロトコルでは比較的簡単です。ただし、多くのコントロールプレーンプロトコルはマルチキャストトラフィックを使用します。たとえば、OSPF、RIP、PIMなどです。完全なリストについては、IANAのIPv4マルチキャストアドレス空間レジストリを参照してください。

これらのプロトコルには、Routing Information Protocol（RIP；ルーティング情報プロトコル）やEnhanced Interior Group Routing Protocol(EIGRP)などの認証機能が組み込まれているものもあれば、IPSecに依存してこの認証を提供するものもあります（OSPFv3、PIMなど）。 後者の場合、GET VPNはこれらのプロトコルを保護するためのスケーラブルな方法を提供します。ほとんどの場合、必要なのはプロトコルメッセージ認証、つまり信頼できるピアからメッセージが送信されたかどうかの確認です。ただし、GET VPNではこのようなメッセージの暗号化も可能です。

このようなコントロールプレーントラフィックを保護（通常は認証のみ）するには、トラフィックをACLで記述し、GET VPNポリシーに含める必要があります。詳細は、保護するプロトコルによって異なります。ここでは、ACLに入力GET VPNノード（カプセル化されている）のみを通過するトラフィックが含まれているか、または出力ノードも通過するかについて注意する必要があります。

PIMプロトコルを保護する基本的な方法は2つあります。

- **permit ip any 224.0.0.13 0.0.0.0**:これは「すべてのPIMルータ」マルチキャストグループです。ただし、ユニキャストPIMメッセージは保護されません
- **permit pim any any**:これにより、マルチキャストとユニキャストのどちらが使用されているかにかかわらず、PIMプロトコルが保護されます

> **注**：これらのコマンドは、概念を説明するための例として提供されています。たとえば、PIMのブートストラップに使用される特定のPIMプロトコル（BSRやAuto-RPなど）を除外する必要があります。導入に依存する利点や不便な点がある方法はありません。詳細については、GET VPNでPIMを保護する方法に関する特定の資料を参照してください。

まとめ

マルチキャストは、ネットワークでますます一般的なサービスになっています。住宅/家庭用ブロードバンドネットワークでのIPTVサービスの出現と、世界の多くの金融市場での電子取引アプリケーションへの移行は、マルチキャストを絶対要件にする要件の2つの例にすぎません。マルチキャストには、設定、運用、管理に関するさまざまな課題があります。重要な課題の1つはセキュリティです。

このドキュメントでは、マルチキャストを保護するさまざまな方法について説明しました。

- 最初に、マルチキャスト制御プレーンとデータプレーン全体を見て、ユニキャストとの違いによって新しいセキュリティの課題がどのように生じるのかを説明します。
- 次に、マルチキャストネットワークで使用される主要なプロトコル、特にIGMP、PIM、およびMSDPについて詳しく調べました。それぞれのケースで、セキュリティ上の脅威の説明と、これらの脅威に対する緩和のための推奨ベストプラクティスが提供されました。
- さらに、特定のビデオフローに必要な帯域幅の量と比較して帯域幅を制限できるブロードバンドエッジネットワークなど、特定のアプリケーションでマルチキャストを保護する方法の特定の例も示します。
- 最後に、GET VPNアーキテクチャは、セキュアなVPNを配信するためのIPSecを使用した統合マルチキャストの手段として説明されました。

マルチキャストセキュリティを念頭に置いて、ユニキャストとの違いを覚えておいてください。マルチキャスト送信はダイナミックステートの作成に基づいて行われ、マルチキャストではダイナミックパケットレプリケーションが行われ、マルチキャストではPIM JOIN/PRUNEメッセージに応答して単方向ツリーが構築されます。この環境全体のセキュリティには、Cisco IOSコマンドの豊富なフレームワークの理解と導入が含まれます。これらのコマンドの大部分は、CoPPなどのパケットに対して配置されるプロトコル動作、状態（マルチキャスト）、またはポリサーの保護に集中しています。これらのコマンドを正しく使用することで、IPマルチキャストに対して堅牢な保護サービスを提供できます。

要約すると、このドキュメントでは次のような複数のアプローチについて説明しています。

1. SSMの広範な使用：これは(S,G)フォワーディングの使用も可能にする最も単純なPIMモードです。
2. ASMサービスが必要な場合は、堅牢なサービスを提供できることを確認します。静的に定義されたRPを使用すると、動的なRPアナウンスよりも安全なコントロールプレーンが提供されます。Auto-RPとBSRの方が柔軟性が高い
3. PIM-SMが有効になっている場合は、RPへのRegister Tunnelなどの特定の脆弱性の領域を調べ、DRが常に適切に保護されていることを確認します。CoPPはこれらの分野で非常に役立ちます。
4. ドメイン間ASMサービスが必要な場合は、BiDir PIMを導入できるかどうかを検討します。
5. グローバルなmroute/igmpステート制限を使用する：通常の状況および最悪の状況で必要な予想される最大状態とともに、プラットフォームの機能を理解します。プラットフォームの機能内で制限を設定し、ネットワークが最大限の制限まで動作できるようにします。
6. 基本フィルタ：rACL/CoPPおよびインフラストラクチャACL。アクセスレイヤでPIMをブロックします。

IPマルチキャストは、さまざまなアプリケーションサービスを提供するためのエキサイティングでスケーラブルな手段です。ユニキャストと同様に、さまざまなエリアでセキュリティを確保する必要があります。このドキュメントでは、IPマルチキャストネットワークの保護に使用できる基本的な構成要素について説明します。

関連情報

- エンタープライズIPマルチキャストアドレス割り当てのガイドライン
- IPv4 IGMPフィルタの設定
- Group Encrypted Transport VPN

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。