Sichere IP-Multicast-Bereitstellungen

Inhalt

Einleitung

Dieses Dokument beschreibt allgemeine Richtlinien zu Best Practices für den Schutz einer IP-Multicast-Netzwerkinfrastruktur.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IP-Multicast

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

In diesem Dokument werden einige grundlegende Konzepte und Begriffe beschrieben und die folgenden Themen behandelt:

- Mechanismen zur Sicherung einer bestimmten Plattform und des Netzwerks im Allgemeinen.
- Alle Modelle für Source Multicast (ASM) und Source Specific Multicast (SSM).
- Multicast Virtual Private Network (MVPN)-Sicherheit.
- Group Encrypted Transport (GET) Virtual Private Network (VPN)-Architektur zur

Gewährleistung der Vertraulichkeit und Integrität des Datenverkehrs auf Multicast- oder Kontrollebene.

Terminologie

Im IP-Multicast gibt es zwei klassische Servicemodelle:

1. Any Source Multicast (ASM)

2. Source Specific Multicast (SSM)

In ASM wird der Empfänger über einen IGMP- (Internet Group Membership Protocol) oder MLD-Mitgliedschaftsbericht (Multicast Listener Discovery) zu einer Gruppe G hinzugefügt, um die Gruppe anzugeben. In diesem Bericht wird Datenverkehr angefordert, der von einer beliebigen Quelle an die Gruppe G gesendet wird, und somit der Name "any source". In SSM hingegen schließt sich der Empfänger einem bestimmten Kanal an, der durch eine Quelle S definiert ist, die an eine Gruppe G sendet. Jedes dieser Dienstmodelle wird nachfolgend näher beschrieben.

Beliebiges Quell-Multicast

Das ASM-Modell ist durch zwei Protokollklassen gekennzeichnet: "Dense Mode Flood-and-Prune" und "Sparse Mode Explicit Join":

i) Flood-and-Prune-Protokolle mit dichtem Modus (DVMRP/MOSPF/PIM-DM)

Bei Protokollen im Dense-Modus erkennen alle Router im Netzwerk alle Trees, ihre Quellen und Empfänger. Protokolle wie das Distance Vector Multicast Routing Protocol (DVMRP) und das Protocol Independent Multicast (PIM) Dense Mode übertragen "Active Source"-Informationen über das gesamte Netzwerk und erstellen Trees durch die Erstellung von "Prune State" in Teilen der Topologie, in denen der Datenverkehr für einen bestimmten Tree unerwünscht ist. Sie werden auch als Flood-and-Prune-Protokolle bezeichnet. In Multicast Open Shortest Path First (MOSPF) werden Informationen zu Empfängern durch das gesamte Netzwerk geleitet, um die Erstellung von Bäumen zu unterstützen.

Protokolle für den dichten Modus sind unerwünscht, da jeder in einem Teil des Netzwerks erstellte Tree immer die Ressourcennutzung (mit Auswirkungen auf die Konvergenz) auf allen Routern im Netzwerk (oder, falls konfiguriert, innerhalb des administrativen Bereichs) verursachen kann. Diese Protokolle werden im weiteren Verlauf dieses Artikels nicht näher erläutert.

ii) Explizite Verbindungsprotokolle im Sparse-Mode (PIM-SM/PIM-BiDir)

Bei expliziten Zusammenführungsprotokollen im Sparse-Mode erzeugen Geräte keinen gruppenspezifischen Zustand im Netzwerk, es sei denn, ein Empfänger hat einen expliziten IGMP/MLD-Mitgliedschaftsbericht (oder "Join") für eine Gruppe gesendet. Diese ASM-Variante lässt sich gut skalieren und ist das Multicast-Paradigma des Fokus.

Dies ist die Grundlage für den PIM-Sparse-Mode, den die meisten Multicast-Bereitstellungen bisher verwendet haben. Dies ist auch die Grundlage für das bidirektionale PIM (PIM-BiDir), das zunehmend für VIELE Anwendungen (Quellen) zu VIELEN Anwendungen (Empfängern) bereitgestellt wird.

Diese Protokolle werden als Sparse-Mode bezeichnet, da sie IP-Multicast-Bereitstellungsbäume mit einer "spärlichen" Empfängerpopulation effizient unterstützen und einen Status auf der Kontrollebene nur auf Routern im Pfad zwischen Quellen und Empfängern und im PIM-SM/BiDir, dem Rendezvous Point (RP), erstellen. In anderen Teilen des Netzwerks wird niemals ein Zustand erzeugt. Der Status eines Routers wird nur dann explizit erstellt, wenn er einen Join von einem Downstream-Router oder -Empfänger erhält. Daher wird der Name "Explicit Join Protocols" (Explizite Join-Protokolle) verwendet.

Sowohl PIM-SM als auch PIM-BiDir verwenden "SHARED TREES", um die Weiterleitung von Datenverkehr von einer beliebigen Quelle an einen Empfänger zu ermöglichen. Der Multicast-Status in einem Shared Tree wird als (*,G)-Status bezeichnet, wobei das * für JEDE QUELLE ein Platzhalter ist. Darüber hinaus unterstützt PIM-SM die Erstellung eines Status, der sich auf den Datenverkehr von einer bestimmten Quelle bezieht. Diese werden als SOURCE TREES bezeichnet, und der zugehörige Status wird als (S,G)-Status bezeichnet.

Source-Specific Multicast

SSM ist das Modell, das verwendet wird, wenn der Empfänger (oder ein Proxy) "Joins" sendet (S,G), um anzuzeigen, dass er Datenverkehr empfangen möchte, der von der Quelle S an Gruppe G gesendet wird. Dies ist mit IGMPv3/MLDv2-Mitgliedschaftsberichten im "INCLUDE"-Modus möglich. Dieses Modell wird als SSM-Modell (Source-Specific Multicast) bezeichnet. SSM erfordert die Verwendung eines Explicit-Join-Protokolls zwischen Routern. Das Standardprotokoll hierfür ist PIM-SSM, das einfach die Teilmenge von PIM-SM ist, die zum Erstellen von (S,G)-Bäumen verwendet wird. In SSM gibt es keine Shared Trees (*,G).

Multicast-Empfänger können somit einer ASM-Gruppe G "beitreten" oder einem SSM-Kanal (S,G) "beitreten" (oder genauer gesagt "abonnieren"). Um eine Wiederholung des Begriffs "ASM-Gruppe oder SSM-Kanal" zu vermeiden, wird der Begriff (Multicast)-Fluss verwendet, was bedeutet, dass es sich bei dem Fluss um eine ASM-Gruppe oder einen SSM-Kanal handeln könnte.

Relevante Multicast-Protokolle/-Pakettypen

Zum Sichern eines Multicast-Netzwerks ist es wichtig, die gängigen Pakettypen zu kennen und sich vor diesen zu schützen. Es gibt drei Hauptprotokolle, die betroffen sein sollten:

1. IGMP/MLD
2. PIM
3. MSDP

Im nächsten Abschnitt werden diese Protokolle und die damit verbundenen Probleme behandelt.

IGMP-/MLD-Pakete

IGMP/MLD ist das Protokoll, das von Multicast-Empfängern verwendet wird, um einem Router zu signalisieren, dass sie Inhalte für eine bestimmte Multicast-Gruppe empfangen möchten. Internet

Group Membership Protocol (IGMP) ist das Protokoll, das in IPv4 und Multicast Listener Discovery (MLD) in IPv6 verwendet wird.

Es gibt zwei häufig verwendete IGMP-Versionen: IGMPv2 und IGMPv3. Es gibt auch zwei häufig verwendete MLD-Versionen: MLDv1 und MLDv2.

IGMPv2 und MLDv1 sind funktional äquivalent, IGMPv3 und MLDv2 sind funktional äquivalent.

Diese Protokolle werden in den folgenden Links angegeben:

IGMPv2: RFC 2236

MLDv1: RFC 3590

IGMPv3 und MLDv2: RFC 4604

IGMPv2 und IGMPv3 ist nicht nur ein Protokoll, sondern auch ein IPv4-IP-Protokoll (insbesondere Protokollnummer 2). Es wird nicht nur wie in diesen RFCs beschrieben verwendet, um Multicast-Gruppenmitgliedschaften zu melden, sondern auch von anderen IPv4-Multicast-Protokollen wie DVMRP, PIM Version 1, mtrace und mrinfo. Dies ist wichtig, um sich zu erinnern, wenn Sie versuchen, IGMP zu filtern (z. B. über Cisco IOS® ACLs). Bei IPv6 ist MLD kein IPv6-Protokoll. Stattdessen wird ICMPv6 verwendet, um MLD-Pakete zu übertragen. PIM Version 2 ist der gleiche Protokolltyp in IPv4 und IPv6 (Protokollnummer 103).

PIM-Steuerungspakete

In diesem Abschnitt werden Multicast- und Unicast-PIM-Steuerungspakete behandelt. Auto-RP sowie Bootstrap Router (BSR), mit denen Rendezvous Points ausgewählt und Zuweisungen von Gruppen zu RP in PIM-SM-Netzwerken gesteuert werden können, werden besprochen.

Multicast-PIM-Steuerungspakete

Multicast-PIM-Steuerungspakete umfassen:

- **PIM Hello** - Das PIM Hello-Paket ist ein IP-Multicast-Paket mit lokalem Gültigkeitsbereich, das an einen Router gesendet wird, der mit demselben Netzwerk verbunden ist, um PIM-Nachbarn einzurichten.
- **PIM Join/Prune** - PIM Join/Prunes sind IP-Multicast-Pakete mit lokalem Gültigkeitsbereich, die gesendet werden, um den Multicast-Status zu erstellen/zu entfernen. Sie werden nur an PIM-Nachbarn gesendet. Sie sind Multicast-fähig im LAN, um die Bestätigung, Unterdrückung von Berichten und andere Details des PIM-Protokolls zu erleichtern, werden aber immer an einen bestimmten Nachbarn weitergeleitet.
- **PIM DF-elect** - Der von PIM designierte Forwarder ist der Bi-Dir PIM-Router, der für (*,G) JOINS verantwortlich ist und im Auftrag angeschlossener Empfänger oder nachgeschalteter PIM-Nachbarn an den RP gesendet wird. Wenn ein PIM-Router einen anderen Router erkennt, der (*,G) JOINS für dasselbe Segment für dieselbe Gruppe G sendet, können Sie den Router mit dem besten Pfad zum RP auswählen.
- **PIM-Assert** - PIM-Asserts sind verbindungslokale IP-Multicast-Pakete, die gesendet werden,

wenn ein PIM-Router, der an ein Netzwerksegment angeschlossen ist, das aktiv Pakete für einen bestimmten Punkt (S,G) von einer bestimmten Schnittstelle weiterleitet, beginnt, Pakete für denselben Punkt (S,G) auf derselben Schnittstelle zu EMPFANGEN, an die weitergeleitet wird. Dieses Ereignis zeigt das Vorhandensein eines anderen Routers an, der dies als Single Forwarder (SF) ansieht (S,G). Der Assert-Mechanismus wählt dafür eine eindeutige SF (S,G). Der PIM SF-Router kann Pakete für einen bestimmten (S,G)-Stream weiterleiten. PIM ermöglicht es verschiedenen Routern, die Rolle der SF für verschiedene (S,G) zu übernehmen. Idealerweise ist nur ein SF pro (S,G) vorhanden. Verwechseln Sie SF nicht mit dem designierten Router. Der vom PIM designierte Router ist der Router, der für JOIN/PRUNES- oder SOURCE-REGISTER verantwortlich ist, die an den RP in einem PIM-SM-Netzwerk gesendet werden.
- **PIM-Bootstrap** - PIM-Bootstrap-Nachrichten werden in einem PIMv2-Netzwerk gesendet, um die dynamische Auswahl eines Rendezvous Points für eine bestimmte Gruppe G zu erleichtern.

Unicast-PIM-Steuerungspakete

Unicast-PIM-Steuerungspakete werden vom oder zum RP geleitet und umfassen:

- **Source Register Packet** - PIM Source Register Packets werden gesendet, um eine neue Multicast-Quelle mit einem Rendezvous Point zu registrieren. Sobald eine Quelle beginnt, Multicast-Pakete zu senden, sendet der designierte Router, der mit dem Quellnetzwerk verbunden ist, einen Unicast-Register-Stream an den RP, um anzuzeigen, dass eine aktive Quelle für eine Multicast-Gruppe vorhanden ist, für die der RP zuständig ist.
  Die Quellregisterpakete werden als Unicast-Kapselung des ursprünglichen Multicast-Streams gesendet.
  PIM-Registernachrichten werden auf Prozessebene umgeschaltet und nur gesendet, bis der RP eine Register-Stopp-Nachricht sendet. Die Auswirkungen dieser Pakete auf die Performance sind proportional zur Rate der Quelle (pro (S,G)-Fluss).
- **Register Stopp Packet** - PIM Register Stopp Packets werden vom Rendezvous Point an den PIM DR gesendet, der die Registernachricht gesendet hat. Register Stopp-Nachrichten werden gesendet, sobald der RP anfängt, native Multicast-Pakete von der Quelle zu empfangen.
- **BSR Candidate-Rendezvous Point Advertisement Packet** - PIM BSR C-RP-Advertisement Packets werden an den BSR gesendet, um einen Kandidaten-RP anzukündigen, sobald der BSR gewählt wurde.

Abb. 1: PIM-Unicast-Pakete

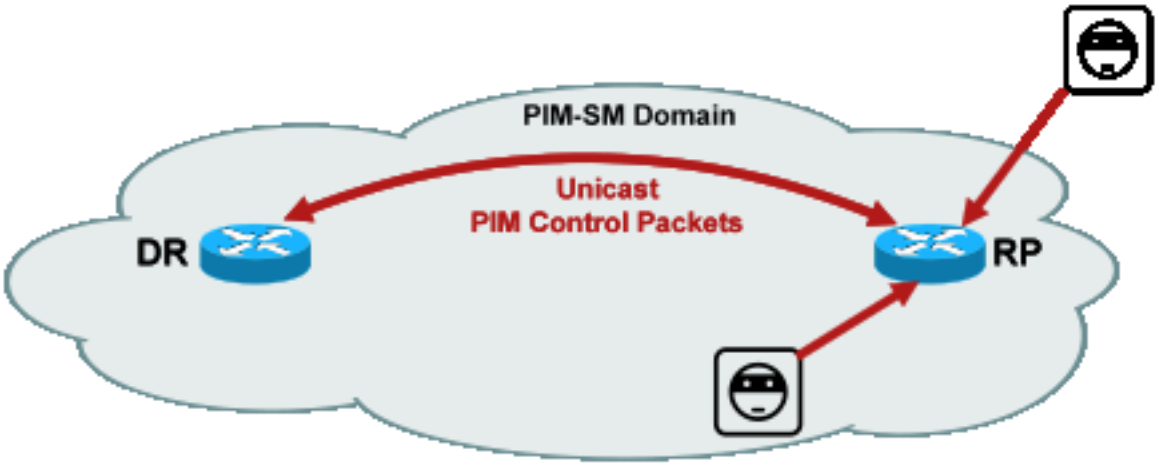

Abb. 1_PIM_Unicast

Angriffe, die solche Pakete ausnutzen, können von überall ausgehen, da es sich bei diesen Paketen um Unicast-Pakete handelt.

Auto-RP-Pakete

Auto-RP ist ein von Cisco entwickeltes Protokoll, das den gleichen Zweck wie PIMv2 BSR erfüllt. Auto-RP wurde vor BSR entwickelt und unterstützt nur IPv4. BSR unterstützt IPv4 und IPv6. Der Mapping Agent in Auto-RP erfüllt die gleiche Funktion wie der Bootstrap-Router in BSR. In BSR werden Nachrichten vom C-RP als Unicast an den Bootstrap-Router gesendet. Bei Auto-RP werden Nachrichten über Multicast an den Mapping-Agent gesendet, wodurch die Filter an den Grenzen vereinfacht werden, wie später beschrieben wird. Eine detaillierte Beschreibung des Auto-RP finden Sie unter folgendem Link: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

In Cisco IOS werden AutoRP-/BSR-Pakete immer weitergeleitet und derzeit nicht deaktiviert. Dies kann bei Auto-RP ein besonderes Sicherheitsrisiko darstellen.

Abb. 2: Auto-RP-Pakete

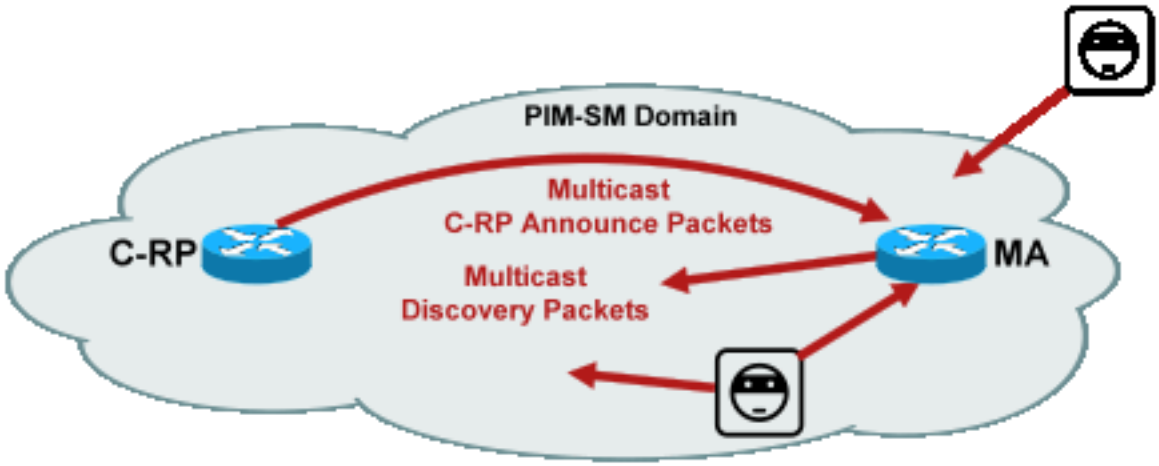

Abb. 2_AutoRP_Pakete

> **Anmerkung:** Obwohl Auto-RP als Mechanismus für die PIM-SM-RP-Ankündigung und -Erkennung verwendet wird, werden keine PIM-Pakete (IP-Protokoll 103) verwendet. stattdessen UDP-Port 496-Pakete mit Multicast-Adressen verwendet.

Vom automatischen RP werden zwei Pakettypen verwendet:

- C-RP-Announce-Pakete: Diese Pakete werden an alle Zuordnungsagenten per Multicast gesendet und verwenden eine Internet Assigned Numbers Authority (IANA), eine reservierte "bekannte" Adresse (224.0.1.39). Sie werden von einem C-RP gesendet, um die RP-Adresse und den Gruppenbereich anzukündigen, für den dieser RP als RP agieren kann.
- C-RP-Erkennungspakete: Diese Pakete werden per Multicast an alle PIM-Router gesendet und verwenden eine IANA-reservierte "bekannte" Adresse (224.0.1.40). Sie werden vom Auto-RP Mapping Agent gesendet, um den spezifischen C-RP anzukündigen, der als RP für einen bestimmten Gruppenbereich ausgewählt ist.

Jeder dieser Pakettypen soll durch das Netzwerk geleitet werden.

In Cisco IOS werden sowohl 224.0.1.39 als auch 224.0.1.40 im PIM Dense Mode weitergeleitet, um zu verhindern, dass der RP einer Gruppe bekannt ist, wenn diese Gruppe zur Verteilung von RP-Informationen verwendet wird. Dies ist die einzige empfohlene Verwendung des PIM Dense Mode.

In Cisco IOS XR sind Auto-RP-Nachrichten Reverse Path Forwarding (RPF)-Flooded Hop by Hop von Neighbor to Neighbor. Daher muss kein PIM DM-Routingstatus erstellt werden, um Auto-RP in Cisco IOS XR zu unterstützen. Tatsächlich bietet Cisco IOS XR überhaupt keine Unterstützung für PIM-DM.

Multicast Service Discovery Protocol (MSDP)-Pakete

MSDP ist das IPv4-Protokoll, mit dem eine Quelle in einer Domäne über ihre jeweiligen Rendezvous Points einem Empfänger in einer anderen Domäne mitgeteilt werden kann. MSDP ist in RFC 3618 festgelegt.

Um Informationen über aktive Quellen zwischen PIM-Domänen auszutauschen, wird MSDP verwendet. Wenn eine Quelle in einer Domäne aktiv wird, stellt MSDP sicher, dass alle Peer-Domänen rechtzeitig von dieser neuen Quelle erfahren, sodass Empfänger in anderen Domänen schnell Kontakt mit dieser neuen Quelle aufnehmen können, wenn sie an eine Gruppe gesendet wurden, an der Empfänger interessiert sind. MSDP wird für die ASM/PIM-SM-Multicast-Kommunikation benötigt und wird über eine Unicast Transport Control Protocol (TCP)-Verbindung ausgeführt, die zwischen Rendezvous Points in den jeweiligen Domänen konfiguriert ist.

Bedrohungen in einer Multicast-Umgebung

Bereiche mit Vertrauen und Vertrauensgrenzen

Dieser Abschnitt des Dokuments ist nach funktionalen Einheiten im Netzwerk organisiert. Das hier behandelte Bedrohungsmodell orientiert sich an diesen Einheiten. In diesem Dokument wird beispielsweise erläutert, wie ein Router in einem Multicast-Netzwerk (aus Multicast-Sicht) unabhängig vom Standort des Routers gesichert werden kann. Ebenso müssen Überlegungen angestellt werden, wie netzwerkweite Sicherheitsmaßnahmen oder -maßnahmen auf einem designierten Router, einem Rendezvous Point usw. implementiert werden können.

Die hier beschriebenen Bedrohungen folgen ebenfalls dieser Logik und sind nach logischen Funktionen im Netzwerk organisiert.

Überblick über Bedrohungen

Auf abstrakter Ebene kann jede Multicast-Bereitstellung einer Reihe von Bedrohungen zu verschiedenen Sicherheitsaspekten ausgesetzt sein. Die wichtigsten Sicherheitsaspekte sind Vertraulichkeit, Integrität und Verfügbarkeit.

- **Bedrohungen der Vertraulichkeit**: In den meisten Anwendungen ist Multicast-Datenverkehr nicht verschlüsselt und kann daher von allen Benutzern über Leitungen oder Netzwerkelemente im Pfad empfangen oder empfangen werden. Im Abschnitt zu GET VPN werden Möglichkeiten zur Verschlüsselung von Multicast-Datenverkehr zur Verhinderung solcher Angriffe erläutert.
- **Bedrohungen für die Integrität des Datenverkehrs**: Ohne Sicherheit auf Anwendungsebene oder netzwerkbasierte Sicherheit wie GET VPN ist Multicast-Datenverkehr anfällig für Änderungen bei der Übertragung. Dies ist besonders wichtig für den Steuerungsebenen-Datenverkehr, der Multicast verwendet, z. B. OSPF, PIM und viele andere Protokolle.
- **Bedrohungen für die Netzwerkintegrität**: Ohne die in diesem Whitepaper beschriebenen Sicherheitsmechanismen können nicht autorisierte Absender, Empfänger oder kompromittierte Netzwerkelemente auf das Multicast-Netzwerk zugreifen und Datenverkehr ohne Autorisierung (Diebstahl des Services) senden und empfangen oder die Netzwerkressourcen überlasten.
- **Bedrohungen für die Verfügbarkeit**: Es gibt eine Reihe von Denial-of-Service-Angriffen, die dazu führen können, dass Ressourcen für legitime Benutzer nicht verfügbar sind.

In den nächsten Abschnitten werden die Bedrohungen für die einzelnen logischen Funktionen im Netzwerk behandelt.

Grundlegende Bedrohungen für einen Router

Es gibt eine Reihe grundlegender Bedrohungen für einen Router, die unabhängig davon auftreten, ob der Router Multicast unterstützt und ob der Angriff Multicast-Datenverkehr oder -Protokolle umfasst.

Denial of Service (DoS)-Angriffe sind die wichtigsten generischen Angriffsvektoren in einem Netzwerk. Im Prinzip kann jedes Netzwerkelement mit einem DoS-Angriff angegriffen werden, wodurch das Element überlastet wird, was zu einem potenziellen späteren Verlust oder einer Verschlechterung des Service für legitime Benutzer führen kann. Es ist äußerst wichtig, die grundlegenden Empfehlungen für die Netzwerksicherheit zu befolgen, die für Unicast gelten.

Es ist zu beachten, dass Multicast-Angriffe nicht immer absichtlich erfolgen, sondern häufig versehentlich erfolgen. Der Witty-Wurm beispielsweise, der erstmals im März 2004 beobachtet wurde, ist ein Beispiel für einen Wurm, der sich durch zufällige Angriffe auf IP-Adressen verbreitete. Infolge der vollständigen Randomisierung des Adressraums wurden auch Multicast-IP-Ziele vom Wurm beeinflusst. In vielen Unternehmen ging die Anzahl der First-Hop-Router zurück, da der Wurm Pakete an viele verschiedene Multicast-Zieladressen schickte. Die Router waren jedoch nicht für eine solche Multicast-Datenverkehrslast ausgelegt, und der zugehörige Status wurde erstellt. Außerdem waren die Ressourcen praktisch erschöpft. Dies zeigt, dass der Multicast-Datenverkehr geschützt werden muss, selbst wenn er in einem Unternehmen nicht verwendet wird.

Allgemeine Bedrohungen für Router:

- Paketüberflutungen jeder Art; z. B. für Hardwarepfade wie langsame Pfade (Punkt-Pfade) und Softwarepfade wie Ports auf Verwaltungs- oder Steuerungsebene, einschließlich Secure Shell (SSH), Telnet, Border Gateway Protocol (BGP), OSPF, Network Time Protocol (NTP) usw.
- Eindringen in den Router mit anschließender Nutzung der Funktionen des Routers schwache Telnet- oder SSH-Passwörter und schwache SNMP-Community-Strings (Simple Network Management Protocol) sind in modernen Netzwerken ein häufiges Problem.
- Betriebliche Probleme wie Fehlkonfigurationen oder Insider-Angriffe können die Sicherheit des gesamten Netzwerks und seines Datenverkehrs gefährden.

Wenn Multicast auf einem Router aktiviert ist, muss es zusätzlich zu Unicast gesichert werden. Die Verwendung von IP-Multicast ändert nichts am grundlegenden Bedrohungsmodell. Sie ermöglicht jedoch zusätzliche Protokolle (PIM, IGMP, MLD, MSDP), die Angriffen ausgesetzt sein könnten und die speziell geschützt werden müssen. Wenn in diesen Protokollen Unicast-Datenverkehr verwendet wird, ist das Bedrohungsmodell mit anderen Protokollen identisch, die vom Router ausgeführt werden.

Dabei ist zu beachten, dass Multicast-Datenverkehr nicht auf die gleiche Weise wie Unicast-

Datenverkehr für Angriffe auf einen Router verwendet werden kann, da Multicast-Datenverkehr grundsätzlich "empfängergesteuert" ist und nicht auf ein entferntes Ziel ausgerichtet werden kann. Ein Angriffsziel muss explizit mit dem Multicast-Stream "verbunden" werden. In den meisten Fällen (Auto-RP ist die wichtigste Ausnahme) empfangen Router nur Multicast-Datenverkehr "link local". Link-lokaler Datenverkehr wird nie weitergeleitet. Daher können Angriffe auf einen Router mit Multicast-Paketen nur von direkt verbundenen Angreifern ausgehen.

Bedrohungen von der Quellseite

Multicast-Quellen, z. B. PCs oder Videoserver, stehen manchmal nicht unter derselben administrativen Kontrolle wie das Netzwerk. Aus Sicht des Netzbetreibers wird der Absender daher meist als nicht vertrauenswürdig behandelt. Angesichts der leistungsstarken Funktionen von PCs und Servern und ihrer komplexen Sicherheitseinstellungen, die häufig unvollständig sind, stellen die Absender eine erhebliche Bedrohung für jedes Netzwerk dar, zu dem auch Multicast gehört. Diese Bedrohungen umfassen:

- **Layer-2-Angriffe**: Auf Layer 2 gibt es eine Vielzahl von Angriffsformen, um verschiedene Arten von Angriffen auszuführen. Diese gelten für Unicast ebenso wie für Multicast. Da diese Angriffsformen nicht spezifisch für Multicast sind, werden sie in diesem Dokument nicht näher erläutert. Weitere Informationen finden Sie im Cisco Press Book "LAN Switch Security", ISBN-10: 1-58705-467-1.
- **Angriffe mit Multicast-Datenverkehr:** Wie bereits beschrieben, ist es schwierig, Angriffe mit Multicast-Datenverkehr durchzuführen, da der First-Hop-Router keinen Multicast-Datenverkehr weiterleitet, es sei denn, es ist ein Listener für die Gruppe vorhanden. Der erste Hop kann jedoch auf verschiedene Weise mit Multicast-Paketen angegriffen werden:
- Netzwerksättigungsangriffe: Ein Angreifer kann ein Segment mit Multicast-Paketen überfluten und dabei die verfügbare Bandbreite überlasten, was zu einem DoS-Zustand führen kann.
- Multicast-Status-Angriffe: Der First-Hop-Router ist mit Multicast-Paketen überschwemmt, die zu viele Zustände verursachen können, was zu einem DoS-Angriff führen kann.
- Ein Absender könnte versuchen, über versendete PIM-Hellos zum PIM DR zu werden. In diesen Fällen wird kein Datenverkehr zum oder vom LAN weitergeleitet.
- PIM DF-Auswahlpakete für einen BiDir-PIM DF konnten gefälscht werden. In diesen Fällen wird kein Datenverkehr zum oder vom LAN weitergeleitet.
- Ein Absender kann AutoRP-Discovery- oder BSR-Bootstrap-Nachrichten als Spoofing verwenden. Dadurch wird ein gefälschter RP gemeldet und ein PIM-SM/BiDir-Service wird deaktiviert oder unterbrochen.
- Ein Absender könnte Unicast-Angriffe wie PIM-Quellregistrierung/Register-Stopp-Nachrichten auslösen oder BSR Announce-Pakete senden und einen gefälschten BSR ankündigen.
- Ein Absender kann an jede gültige Multicast-Gruppe senden, sofern diese nicht gefiltert wird. Wenn eine Quelladresse gefälscht und nicht am Edge verhindert wird, kann der Absender die Quell-IP-Adresse eines legitimen Absenders verwenden und Inhalte in Teilen des Netzwerks überschreiben.
- Multicast-Angriffe auf Kontrollebenenprotokolle: Eine Reihe von Protokollen, die nicht mit Multicast verknüpft sind, wie OSPF und DHCP (Dynamic Host Configuration Protocol), verwenden Multicast-Pakete, die zum Angriff auf diese Protokolle verwendet werden können
- **Masquerading:** Es gibt eine Reihe von Angriffsformen, bei denen ein Absender vorgeben kann, ein anderer Absender zu sein. Gefälschte Quell-IP-Adressen gehören zu diesen

Angriffsformen.

- **Diebstahl des Dienstes:** Sofern die Absender nicht kontrolliert werden, ist es möglich, den Multicast-Dienst unrechtmäßig von der Absenderseite aus zu verwenden.

  Anmerkung: Hosts senden oder empfangen normalerweise keine PIM-Pakete. Host, der dies tut, kann wahrscheinlich einen Angriff versuchen.

Bedrohungen von der Empfängerseite

Der Receiver ist in der Regel auch eine Plattform mit hoher CPU-Leistung und Bandbreite, die eine Reihe von Angriffsformen ermöglicht. Diese sind meist identisch mit den Bedrohungen auf der Absenderseite. Layer-2-Angriffe bleiben ein wichtiger Angriffsvektor. Auch auf Empfängerseite sind gefälschte Empfänger und Diebstahl von Services möglich, mit der Ausnahme, dass der Angriffsvektor typischerweise IGMP (oder Layer-2-Angriffe, wie erwähnt) ist.

Bedrohungen gegen einen Rendezvous Point und BSR

PIM-SM-RPs und PIM-BSRs sind kritische Punkte in einem Multicast-Netzwerk und daher wertvolle Ziele für einen Angreifer. Wenn es sich bei dem First-Hop-Router nicht um einen handelt, können nur Unicast-Angriffsformen, zu denen auch PIM-Unicast gehört, direkt auf diese Elemente ausgerichtet werden. Zu den Bedrohungen für RPs und BSRs gehören:

- Alle allgemeinen Angriffsformen, wie im Abschnitt "Grundlegende Bedrohungen gegen einen Router" beschrieben.
- PIM-Unicast-Angriffe, möglicherweise mit gefälschten Quell-IP-Adressen, ermöglichen DoS-Angriffe. Dabei werden PIM-Registrierungs- oder Register-Stopp-Nachrichten verwendet, die von einem böswilligen Gerät gesendet werden.

Multicast- und Unicast-Sicherheit (verglichen)

Statusüberlegungen/Filter

Betrachten Sie die Topologie in Abbildung 3, die eine Quelle, drei Empfänger (A, B, C), einen Switch (S1) und zwei Router (R1 und R2) zeigt. Die blaue Linie stellt einen Unicast-Stream dar, die rote Linie einen Multicast-Stream. Alle drei Empfänger sind Mitglieder des Multicast-Flusses.

Abb. 3: Replikation in Routern und Switches

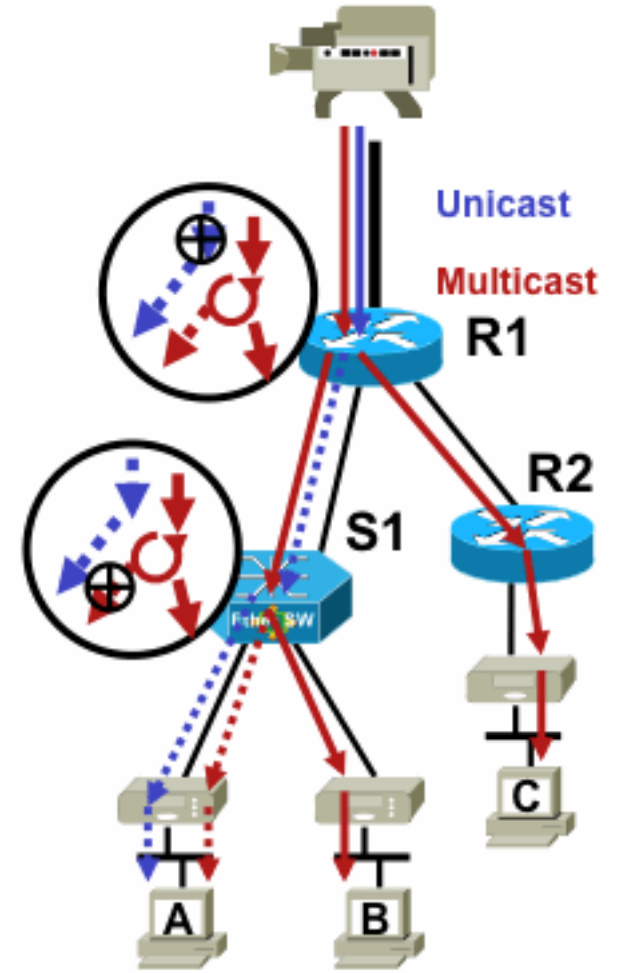

Abb. 3_Replikation_RS

So unterbinden Sie den Datenverkehrsfluss von einer bestimmten Quelle zu einem bestimmten Empfänger:

- Installieren Sie für den Unicast-Stream einen Filter an einer beliebigen Stelle auf dem Pfad von Sender zu Empfänger.
- Für den Multicast-Stream müssen Administratoren jedoch genauer festlegen, wo Filter installiert werden: am empfängerseitigen Filter nach dem letzten Replikationspunkt vor dem Empfänger; auf der Quellseite vor dem ersten Replikationspunkt nach der Quelle filtern.

Angriffe von Multicast-Quellen

Dieser Abschnitt gilt für die ASM- und SSM-Servicemodelle, bei denen die Weiterleitung des Datenverkehrs auf dem Empfang expliziter Joins auf Empfängerseite basiert.

Für Unicast-Streams gibt es keinen impliziten Empfängerschutz. Eine Unicast-Quelle kann Datenverkehr an ein Ziel senden, selbst wenn dieses Ziel nicht nach dem Datenverkehr gefragt hat. Daher werden Abwehrmechanismen wie Firewalls in der Regel verwendet, um Endpunkte zu schützen. Multicast dagegen verfügt über einen gewissen impliziten Schutz, der in die Protokolle integriert ist. Der Datenverkehr erreicht idealerweise nur einen Empfänger, der sich dem betreffenden Datenfluss angeschlossen hat.

Mit ASM können Quellen Datenverkehr einfügen oder DoS-Angriffe durch Multicast-Datenverkehrsübertragung an eine beliebige Gruppe starten, die von einem aktiven RP unterstützt wird. Idealerweise wird dieser Datenverkehr nicht an einen Empfänger weitergeleitet, sondern kann mindestens den First-Hop-Router im Pfad sowie den RP erreichen, was begrenzte Angriffe ermöglicht. Wenn eine böswillige Quelle jedoch eine Gruppe kennt, an der ein Empfänger interessiert ist, und keine geeigneten Filter vorhanden sind, kann sie Datenverkehr an diese Gruppe senden. Dieser Datenverkehr wird empfangen, solange die Empfänger die Gruppe überwachen.

Mit SSM sind Angriffe unerwünschter Quellen nur auf dem First-Hop-Router möglich, an dem der Datenverkehr gestoppt wird, wenn kein Empfänger diesem (S,G)-Kanal beigetreten ist. Dies führt zu keinem Zustandsangriff auf den First-Hop-Router, da der gesamte SSM-Datenverkehr, für den kein expliziter Join-Zustand besteht, von den Empfängern verworfen wird. Bei diesem Modell reicht es nicht aus, dass eine böswillige Quelle weiß, an welcher Gruppe ein Ziel interessiert ist, da "Joins" quellenspezifisch sind. In diesem Fall wären gefälschte IP-Quelladressen sowie potenzielle Routing-Angriffe erforderlich.

Statusangriffe

Selbst ohne Empfänger in einem Netzwerk erstellt PIM-SM den Status (S,G) und (*,G) auf dem der Quelle nächstgelegenen First-Hop-Router sowie auf dem Rendezvous Point. Somit besteht die Möglichkeit eines State-Angriffs auf das Netzwerk am Source First-Hop-Router und auf den PIM-SM-RP.

Wenn eine schädliche Quelle beginnt, Datenverkehr an mehrere Gruppen zu senden, dann erzeugen die Router im Netzwerk für jede erkannte Gruppe einen Status an der Quelle und am RP, vorausgesetzt, die betreffenden Gruppen sind gemäß der RP-Konfiguration zulässig.

Daher ist PIM-SM Status- und Datenverkehrsangriffen von Quellen ausgesetzt. Der Angriff kann noch verstärkt werden, wenn die Quelle ihre Quell-IP-Adresse innerhalb des richtigen Präfix zufällig ändert, d. h. wenn nur die Host-Bits der Adresse gefälscht werden.

Abb. 4: ASM RP-Angriffe

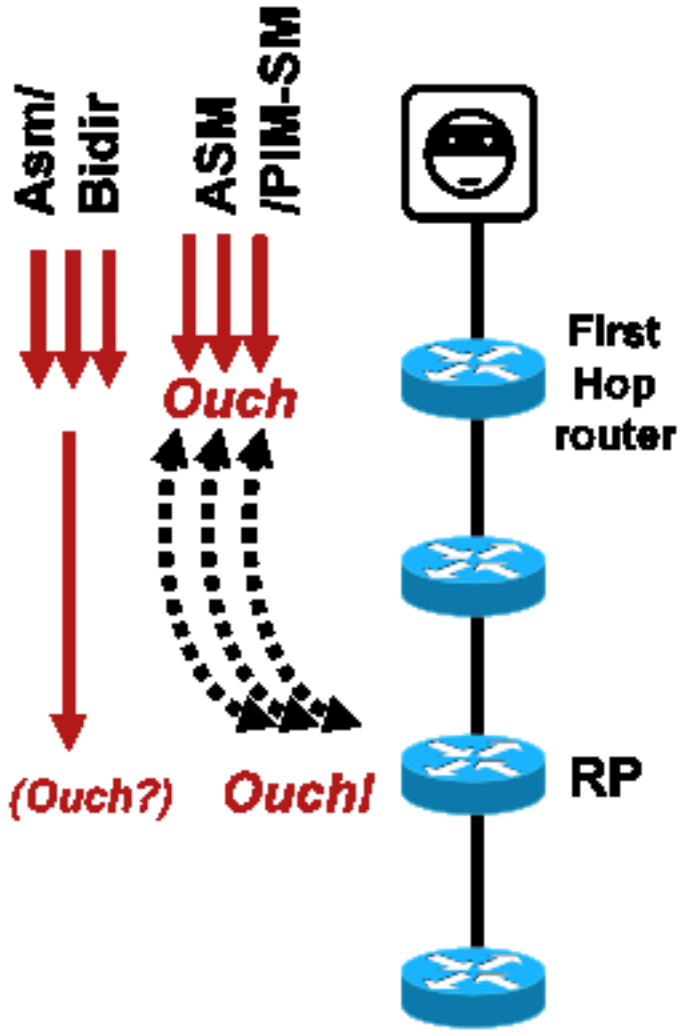

Abb. 4_ASM_RP_Angriffe

Wie bei PIM-SSM sind PIM-BiDir-Angriffe zur Erstellung des Status von Quellen nicht möglich. Der Datenverkehr in PIM-BiDir wird sowohl nach einem durch Joins von Empfängern erstellten Zustand als auch nach einem durch den Zustand weitergeleiteten Datenverkehr an den RP weitergeleitet, sodass er Empfänger hinter dem RP erreichen kann, da die Joins nur an den RP weitergeleitet werden. Der Status "State-to-Forwarding" (Status von Status zu Weiterleitung) zum RP wird als Status (*,G/M) bezeichnet und durch die RP-Konfiguration (statisch, Auto-RP, BSR) erstellt. Es ändert sich nicht, wenn Quellen vorhanden sind. Aus diesem Grund können Angreifer Multicast-Datenverkehr an einen PIM-BiDir-RP senden. Im Gegensatz zu PIM-SM ist ein PIM-BiDir-RP jedoch keine "aktive" Einheit, sondern leitet oder verwirft lediglich Datenverkehr für PIM-BiDir-Gruppen weiter.

> **Anmerkung:** Auf einigen Cisco IOS-Plattformen (*,G/M) wird der Status nicht unterstützt. In solchen Fällen können Quellen den Router durch Multicast-Datenverkehrsübertragung an mehrere PIM-BiDir-Gruppen angreifen, was zur Erstellung eines (*,G)-Status führt. Beispielsweise unterstützt der Catalyst 6500-Switch (*,G/M)-Status.

Vom Empfänger ausgelöste Angriffe

Angriffe können von Multicast-Empfängern ausgehen. Jeder Empfänger, der IGMP-/MLD-Berichte

sendet, erzeugt normalerweise einen Status auf dem First-Hop-Router. Es gibt keinen entsprechenden Mechanismus in Unicast.

Abb. 5: Explizite Join-basierte Datenweiterleitung auf Empfängerseite

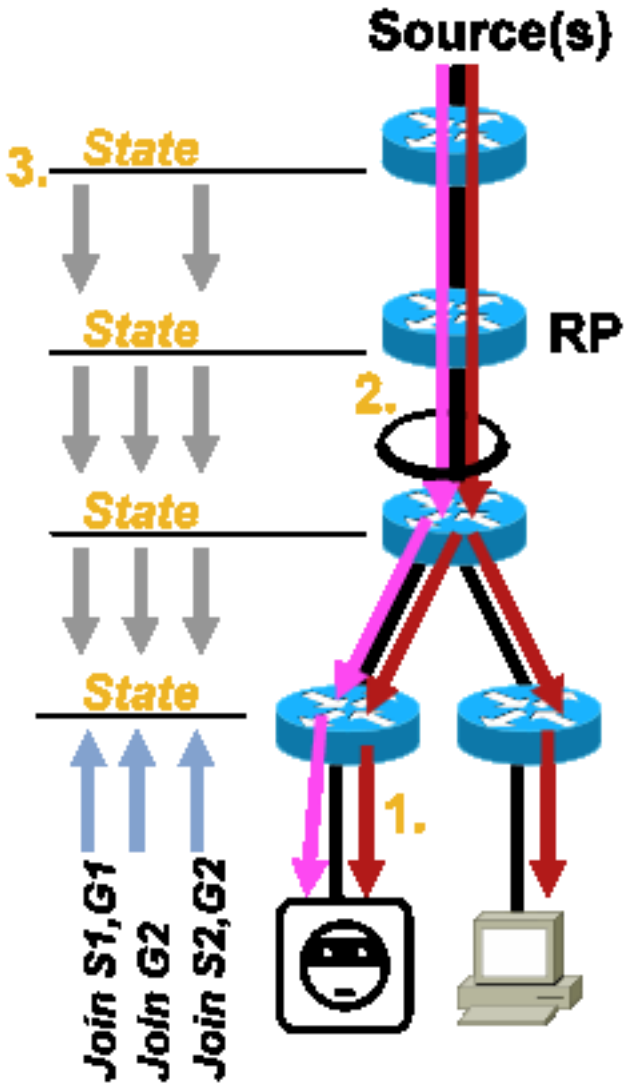

Abb. 5_Empfänger_Explicit_Join

Es gibt drei Arten von Empfängerangriffen:

1. Ein Multicast-Empfänger kann versuchen, einem Fluss beizutreten, für den er nicht autorisiert ist, und versuchen, Inhalte zu empfangen, für die er nicht autorisiert ist.
2. Ein Multicast-Empfänger kann die verfügbare Netzwerkbandbreite durch Interesse an vielen Gruppen oder Kanälen überlasten. Diese Art von Angriff wird zu einem Angriff mit gemeinsam genutzter Bandbreite gegen andere potenzielle Empfänger von Inhalten.
3. Ein Multicast-Empfänger kann versuchen, einen Angriff auf Router oder Switches zu starten. Es kann eine große Anzahl von IGMP-Berichten generiert werden, was zu einem großen Anteil an Multicast-Tree-Status und einer möglichen Überlastung der Routerkapazität führen kann. Dies wiederum kann die Multicast-Konvergenzzeiten erhöhen oder zu einem DoS auf dem Router führen.

Im nächsten Abschnitt, Security within a Multicast Network (Sicherheit in einem Multicast-Netzwerk), werden verschiedene Möglichkeiten zur Abwehr dieser Art von Angriffen beschrieben.

Sicherheit in einem Multicast-Netzwerk

Netzwerkelementsicherheit

Sicherheit ist keine isolierte Funktion, sondern fester Bestandteil jedes Netzwerkdesigns. Daher muss die Sicherheit an jedem Punkt im Netzwerk berücksichtigt werden. Es ist äußerst wichtig, dass jedes Netzwerkelement angemessen geschützt ist. Ein mögliches Angriffsszenario, das auf jede Technologie anwendbar ist, ist ein Router, der von einem Eindringling unterwandert wird. Sobald ein Eindringling die Kontrolle über einen Router hat, kann der Angreifer eine Reihe verschiedener Angriffsszenarien ausführen. Jedes Netzwerkelement muss daher angemessen vor jeder Form von einfachem Angriff sowie vor bestimmten Multicast-Angriffen geschützt werden.

Control Plane Policing (CoPP)

CoPP ist die Weiterentwicklung von Router-ACLs (rACLs) und auf den meisten Plattformen verfügbar. Das Prinzip ist dasselbe: Nur der an den Router gerichtete Datenverkehr wird von CoPP geregelt.

Die Service-Richtlinie verwendet dieselbe Syntax wie alle Quality-of-Service-Richtlinien mit Richtlinienzuordnungen und Klassenzuordnungen. Daher wird die Funktionalität von rACLs (Zulassen/Verweigern) mit Ratenlimitierungen für bestimmten Datenverkehr in Richtung Steuerungsebene erweitert.

> **Anmerkung:** Bei bestimmten Plattformen, z. B. Switches der Catalyst Serie 9000, ist CoPP standardmäßig aktiviert, und der Schutz wird nicht ersetzt. Weitere Informationen finden Sie im CoPP-Handbuch.

Wenn Sie sich entscheiden, rACLS oder CoPP in einem Live-Netzwerk anzupassen, zu ändern oder zu erstellen, müssen Sie vorsichtig sein. Da beide Funktionen den gesamten Datenverkehr zur Steuerungsebene filtern können, müssen alle erforderlichen Protokolle der Kontroll- und Verwaltungsebene explizit zugelassen werden. Die Liste der erforderlichen Protokolle ist groß, und es kann leicht sein, weniger offensichtliche Protokolle wie Terminal Access Controller Access Control System (TACACS) zu übersehen. Alle nicht standardmäßigen rACL- und CoPP-Konfigurationen müssen vor der Bereitstellung in Produktionsnetzwerken immer in einer Laborumgebung getestet werden. Darüber hinaus müssen Erstbereitstellungen nur mit einer Richtlinie für die Genehmigung beginnen. Dies ermöglicht die Validierung unerwarteter Treffer mit Zugriffskontrolllisten-Zählern.

In einer Multicast-Umgebung müssen die erforderlichen Multicast-Protokolle (PIM, MSDP, IGMP usw.) in rACL oder CoPP zugelassen werden, damit Multicast ordnungsgemäß funktioniert. Denken Sie daran, dass das erste Paket in einem Multicast-Stream von der Quelle in einem PIM-SM-Szenario als Paket auf der Kontrollebene verwendet wird, um den Multicast-Status auf der Kontrollebene des Geräts zu erstellen. Daher müssen relevante Multicast-Gruppen in rACL oder CoPP zugelassen werden. Da es eine Reihe von plattformspezifischen Ausnahmen gibt, ist es wichtig, vor der Bereitstellung die entsprechende Dokumentation zu konsultieren und alle

geplanten Konfigurationen zu testen.

Local Packet Transport Service (LPTS)

Auf Cisco IOS XR dient der Local Packet Transport Service (LPTS) ähnlich wie CoPP auf Cisco IOS als Überwachung des Datenverkehrs zur Steuerungsebene des Routers. Außerdem kann der Empfangsdatenverkehr, der Unicast- und Multicast-Datenverkehr umfasst, gefiltert und der Übertragungsrate eingeschränkt werden.

Multicast-spezifische Sicherheit

In einem Multicast-fähigen Netzwerk muss jedes Netzwerkelement mit Multicast-spezifischen Sicherheitsfunktionen gesichert werden. Diese werden in diesem Abschnitt für einen allgemeinen Router-Schutz beschrieben. Funktionen, die nicht auf jedem Router, sondern nur an bestimmten Standorten im Netzwerk erforderlich sind, und Funktionen, die eine Interaktion zwischen Routern erfordern (z. B. PIM-Authentifizierung), werden im nächsten Abschnitt behandelt.

Routengrenzwerte

Mit dem Befehl mroute limit wird die Anzahl der Multicast-Routen auf einem Router global begrenzt, und DoS-Angriffe werden verhindert.

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

Abb. 6: Routengrenzwerte

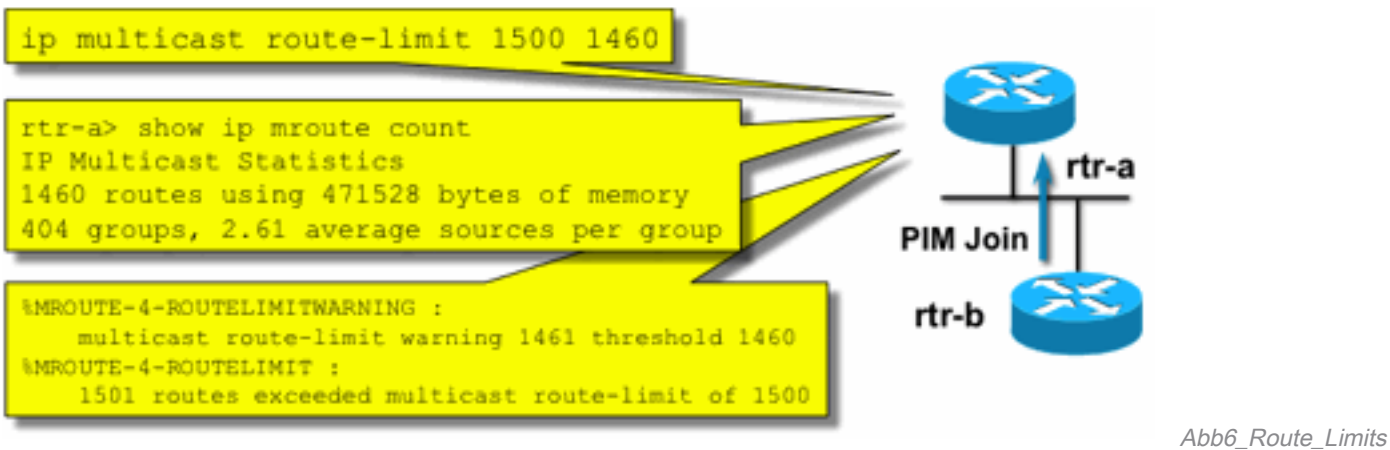

Abb6_Route_Limits

Routinglimits ermöglichen das Festlegen eines Grenzwerts für die Anzahl von Routen, die in die Multicast-Routing-Tabelle aufgenommen werden dürfen. Wenn ein Grenzwert für die Multicast-Route aktiviert ist, wird kein Multicast-Status erstellt, der über den konfigurierten Grenzwert hinausgeht. Außerdem gibt es eine Warnschwelle. Wenn die Anzahl der Routen den Warnschwellenwert überschreitet, werden Syslog-Warnmeldungen ausgelöst. An der Routengrenze werden alle weiteren Pakete verworfen, die den Status auslösen würden.

Der Befehl **ip multicast route-limit** ist ebenfalls pro MVRF verfügbar.

Deaktivieren von SAP Listen: no ip sap listen

Der Befehl **sap listen** veranlasst, dass ein Router Session Announcement Protocol/Session Description Protocol (SAP/SDP)-Nachrichten empfängt. SAP/SDP ist ein Legacy-Protokoll, das aus den Tagen des Multicast-Backbone (MBONE) stammt. Diese Meldungen enthalten Verzeichnisinformationen zu Multicast-Inhalten, die künftig oder aktuell verfügbar sind. Dies kann eine DoS-Quelle für die CPU und die Speicherressourcen des Routers sein, und diese Funktion muss daher deaktiviert werden.

Kontrolle des Zugriffs auf mrinfo-Informationen - der Befehl "ip multicast mrinfo-filter"

Der Befehl mrinfo (unter Cisco IOS und einigen Versionen von Microsoft Windows und Linux verfügbar) verwendet verschiedene Nachrichten, um Informationen von einem Multicast-Router abzufragen. Der globale Konfigurationsbefehl **ip multicast mrinfo-filter** kann verwendet werden, um den Zugriff auf diese Informationen auf eine Untergruppe von Quellen zu beschränken oder sie vollständig zu deaktivieren.

In diesem Beispiel werden Abfragen aus 192.168.1.1 abgelehnt, während Abfragen aus einer anderen Quelle zulässig sind:

```
ip multicast mrinfo-filter 51

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

In diesem Beispiel wird *Marinade* Anfragen aus allen Quellen:

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

> **Anmerkung:** Wie bei jeder ACL bedeutet *deny*, dass das Paket gefiltert wird, während *permit* bedeutet, dass das Paket zulässig ist.

Wenn der Befehl **mrinfo** für Diagnosezwecke verwendet wird, wird dringend empfohlen, den Befehl **ip multicast mrinfo-filter** mit einer geeigneten ACL zu konfigurieren, um Abfragen nur von einer Teilmenge der Quelladressen zuzulassen. Die Informationen aus dem Befehl *mrinfo* können auch über SNMP abgerufen werden. Vollständige Blöcke von mrinfo-Anfragen (blockieren Sie jede Quelle von Abfragen des Geräts) wird dringend empfohlen.

Netzwerksicherheit

In diesem Abschnitt werden verschiedene Möglichkeiten zum Sichern von PIM-Multicast- und Unicast-Kontrollpaketen sowie von Auto-RP und BSR erörtert.

Multicast-Gruppen deaktivieren

Mit den Befehlen **ip multicast group-range/ipv6 multicast group range** können alle Vorgänge für Gruppen deaktiviert werden, die von der ACL abgelehnt wurden:

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

Wenn Pakete für eine der von der ACL abgelehnten Gruppen vorhanden sind, werden sie in allen Steuerungsprotokollen, einschließlich PIM, IGMP, MLD, MSDP, verworfen und auch auf der Datenebene verworfen. Daher werden für diese Gruppenbereiche niemals IGMP/MLD-Cache-Einträge, PIM, Multicast Routing Information Base/Multicast Forwarding Information Base (MRIB/MFIB)-Status erstellt, und alle Datenpakete werden sofort verworfen.

Diese Befehle werden in die globale Konfiguration des Geräts eingegeben.

Es wird empfohlen, diesen Befehl auf allen Routern im Netzwerk bereitzustellen, wenn und soweit verfügbar, damit der gesamte Multicast-Verkehr, der von außerhalb des Netzwerks stammt, kontrolliert wird. Beachten Sie, dass sich diese Befehle auf die Daten- und die Kontrollebene auswirken. Sofern verfügbar, bietet dieser Befehl eine umfassendere Abdeckung als Standard-ACLs und wird bevorzugt.

PIM-Sicherheit

PIM Neighbor Control

Ein PIM-Router muss PIM Hellos empfangen, um eine PIM-Nachbarschaft aufzubauen. Die PIM-Nachbarschaft ist auch die Grundlage für die Auswahl des designierten Routers (DR) und den DR-Failover sowie für gesendete/empfangene PIM-Join-/Prune-/Assert-Nachrichten.

Abb. 7: PIM Neighbor Control

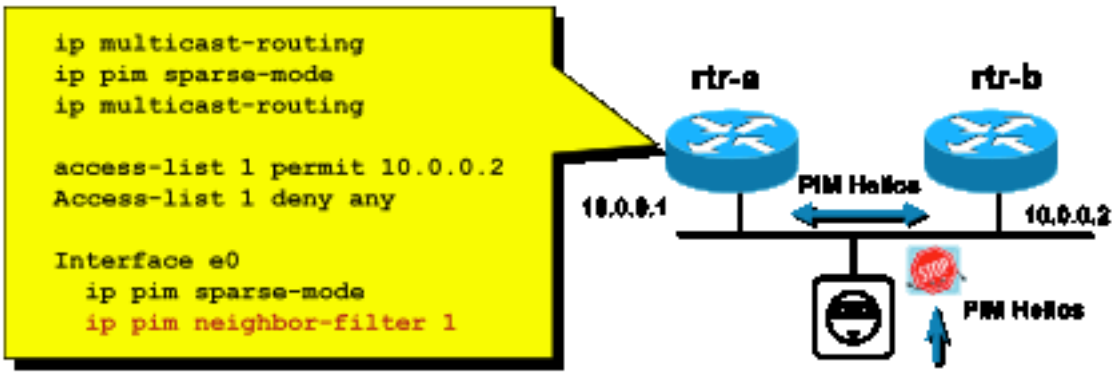

Abb. 7_PIM_neighbor_control

Um unerwünschte Nachbarn zu verhindern, verwenden Sie die **ip pim neighbor-filter** in Abbildung 7 veranschaulicht. Dieser Befehl filtert alle nicht zulässigen Nachbarpakete von PIM-Paketen, darunter Hellos, Join/Prune-Pakete und BSR-Pakete. Hosts auf dem Segment können die Quell-IP-Adresse möglicherweise als PIM-Nachbaradresse angeben. Layer-2-Sicherheitsmechanismen (insbesondere IP Source Guard) sind erforderlich, um zu verhindern, dass Quelladressen von einem Spoofing-Versuch auf einem Segment stammen, oder um PIM-Pakete von Hosts mithilfe einer VLAN-ACL im Access Switch zu verhindern. Das Schlüsselwort "log-input" kann in ACLs verwendet werden, um Pakete zu protokollieren, die mit dem ACE übereinstimmen.

Das PIM-Join/Prune-Paket wird an einen PIM-Nachbarn gesendet, um diesen Nachbarn einem bestimmten (S,G)- oder (*,G)-Pfad hinzuzufügen oder daraus zu entfernen. PIM-Multicast-Pakete sind lokale Multicast-Pakete, die mit einer Time-To-Live (TTL)=1 gesendet werden. Alle diese Pakete sind Multicast an die bekannte All-PIM-Routeradresse: 224.0.0.13. Das bedeutet, dass alle derartigen Angriffe vom gleichen Subnetz ausgehen müssen wie der angegriffene Router. Die Angriffe können gefälschte Hello-, Join/Prune- und Assert-Pakete umfassen.

> **Anmerkung:** Eine künstliche Erhöhung oder Anpassung des TTL-Werts in PIM-Multicast-Paketen auf einen höheren Wert als 1 schafft keine Probleme. Die All-PIM-Router-Adresse wird immer empfangen und lokal auf einem Router behandelt. Es wird niemals direkt von normalen und legitimen Routern weitergeleitet.

Um den RP vor einer potenziellen Flut von PIM-SM-Registernachrichten zu schützen, muss der DR die Anzahl dieser Nachrichten begrenzen. Verwenden Sie den Befehl **ip pim register-rate-limit**:

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

Abb. 8: PIM-SM-Register Tunnelsteuerung

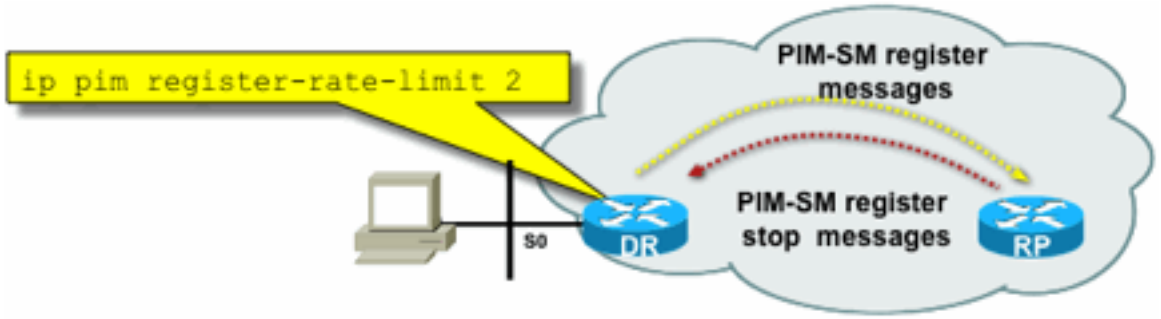

Abb8_PIMSM_Reg Tunnel

PIM-Unicast-Pakete können für Angriffe auf den RP verwendet werden. Daher kann der RP durch Infrastruktur-ACLs vor solchen Angriffen geschützt werden. Denken Sie daran, dass Multicast-Sender und -Empfänger niemals PIM-Pakete senden müssen. Das PIM-Protokoll (IP-Protokoll 103) kann daher in der Regel am Teilnehmer-Edge gefiltert werden.

Automatische RP-Steuerung - RP-Announce-Filter

Der Befehl **ip pim rp-announce filter** ist eine zusätzliche Sicherheitsmaßnahme, die nach Möglichkeit mit Auto-RP konfiguriert werden kann:

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

Dies kann auf dem Zuordnungsagenten konfiguriert werden, um zu steuern, welche Router als Kandidaten-RPs für welche Gruppenbereiche/den Gruppenmodus akzeptiert werden.

Abb. 9: Auto-RP - Filter für RP-Ankündigung

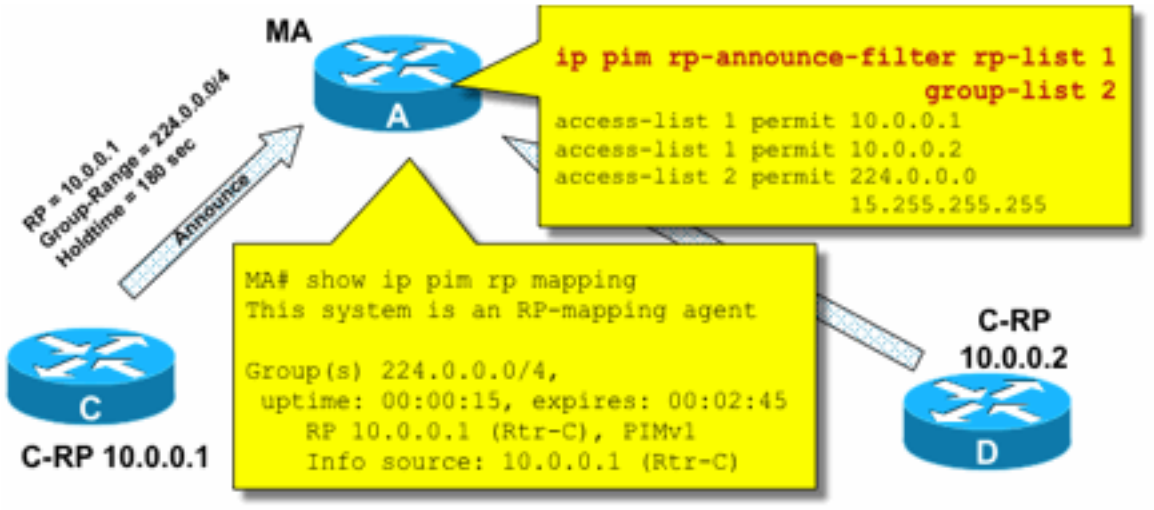

Abb.9_AutoRP_RP_Announce

Automatische RP-Steuerung - Automatische RP-Nachrichten einschränken

Verwenden Sie den Multicast Boundary-Befehl, um AutoRP-Pakete, RP-announce (224.0.1.39) oder RP-discovery (224.0.1.40) auf eine bestimmte PIM-Domäne zu beschränken:

```
ip multicast boundary
```

Abb. 10: Multicast-Grenzbefehl

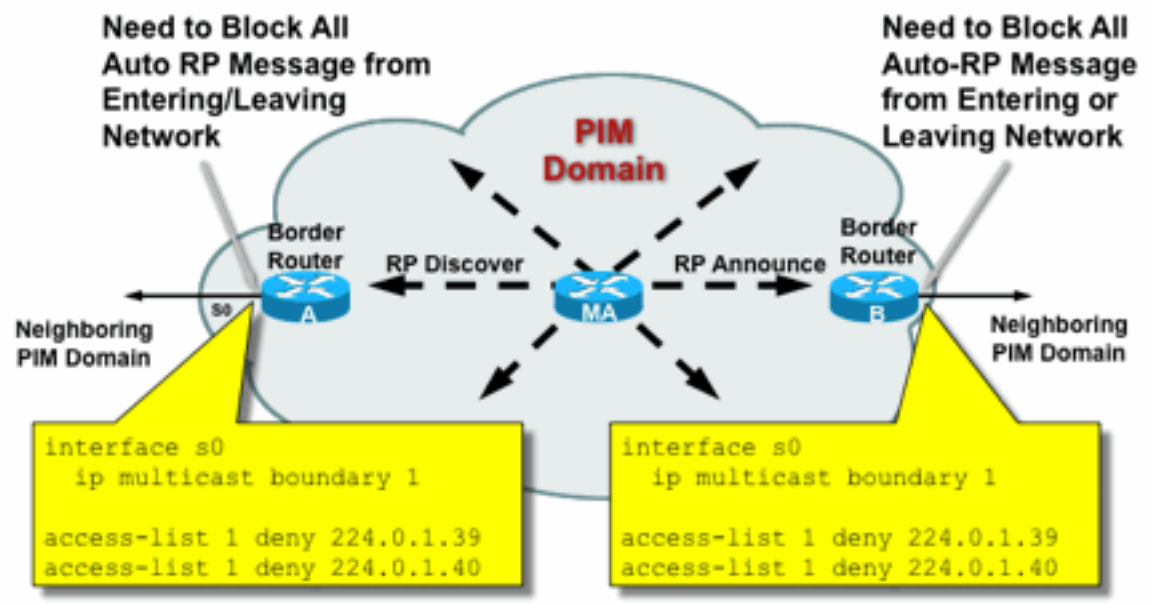

Abb10_Multicast_Boundary

BSR Control - BSR-Nachrichten einschränken

Verwenden Sie **ip pim bsr-border** -Befehl, um BSR-Nachrichten am Rand einer PIM-Domäne zu filtern. Es ist keine ACL erforderlich, da BSR-Nachrichten mit lokalem Link-Multicast "Hop-by-Hop" weitergeleitet werden.

Abb. 11: BSR-Grenze

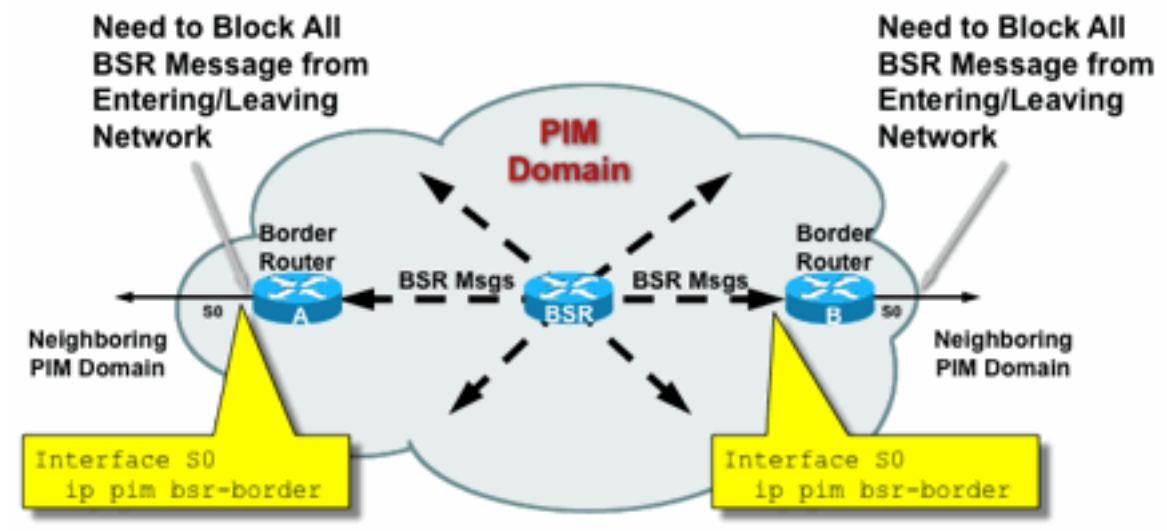

Abb. 11_BSR_Router

RP-/PIM-SM-bezogene Filter

Im letzten Abschnitt werden Filter für Pakete der PIM-SP- und RP-Kontrollebene sowie für Auto-RP-, BSR- und MSDP-Nachrichten behandelt.

Auto-RP-Filter

Abbildung 12 zeigt ein Beispiel für Auto-RP-Filter in Verbindung mit Adressbereichen. Es werden zwei verschiedene Möglichkeiten zum Binden eines Bereichs dargestellt. Die beiden ACLs sind hinsichtlich des automatischen RP identisch.

Abb. 12: Auto-RP-Filter/-Bereiche

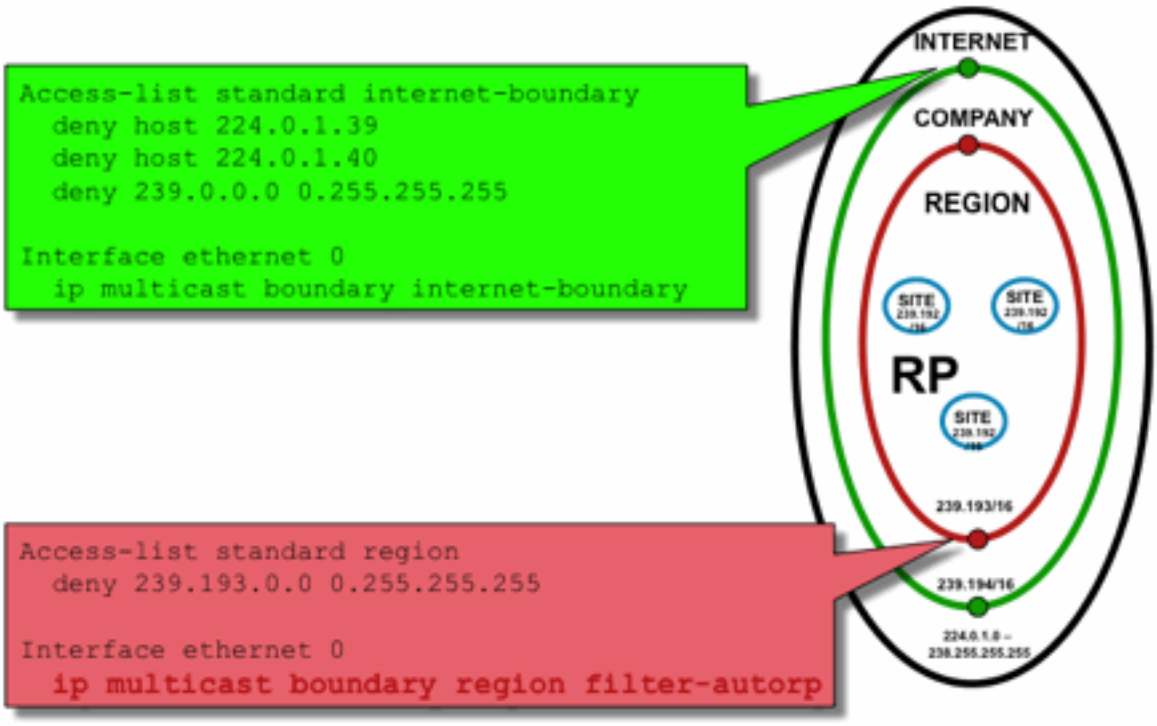

Abb. 12_AutoRP_Filtering_Scoping

Die Grenzflächenfilter für Auto-RP sollen sicherstellen, dass Auto-RP-Ankündigungen nur die Regionen erreichen, die sie unterstützen. Es werden regionale, firmenweite und internetweite Bereiche definiert, in jedem Fall gibt es RPs und Auto-RP-Werbung in jedem Bereich. Administratoren möchten lediglich, dass die regionalen RPs den regionalen Routern bekannt sind, die Unternehmens-RPs den regionalen und Unternehmens-Routern bekannt sind und dass alle Internet-RPs global verfügbar sind. Weitere Bereichsebenen sind möglich.

Wie im Bild gezeigt, gibt es zwei grundlegend verschiedene Möglichkeiten, Auto-RP-Pakete zu filtern: Die Internet-Grenze ruft explizit die Auto-RP-Kontrollgruppen (224.0.1.39 und 224.0.1.40) auf, was zu Filtern für alle Auto-RP-Pakete führt. Diese Methode kann am Edge einer administrativen Domäne verwendet werden, die keine Auto-RP-Pakete durchläuft. Die Regionsgrenze verwendet das Schlüsselwort filter-auto-rp, um eine Untersuchung der Ankündigungen für den rp-to-group-Bereich in Auto-RP-Paketen zu veranlassen. Wenn eine Ankündigung von der ACL explizit abgelehnt wird, wird sie aus dem Auto-RP-Paket entfernt, bevor das Paket weitergeleitet wird. Im Beispiel können so unternehmensweite RPs innerhalb der Regionen bekannt sein, während die regionsweiten RPs an der Grenze von der Region zum Rest des Unternehmens gefiltert werden.

Domänenübergreifende Filter und MSDP

In diesem Beispiel dient ISP1 als PIM-SM-Transitanbieter. Sie unterstützen nur MSDP-Peering mit Nachbarn und akzeptieren nur (S,G), jedoch keinen (*,G)-Datenverkehr auf den Grenzroutern.

In Inter-Domain (in der Regel zwischen autonomen Systemen) sind zwei grundlegende Sicherheitsmaßnahmen zu treffen:

1. Schützen Sie die Datenebene mit dem Befehl **multicast border**. Dadurch wird sichergestellt, dass Multicast-Datenverkehr nur für definierte Gruppen (und möglicherweise Quellen) akzeptiert wird.
2. Schutz des domänenübergreifenden Kontrollebenenverkehrs (MSDP) Es umfasst eine Reihe separater Sicherheitsmaßnahmen: MSDP-Inhaltskontrolle, Statusbeschränkung und Nachbar-Authentifizierung.

Abbildung 13 zeigt eine Beispielkonfiguration eines Schnittstellenfilters auf einem der Grenzrouter von ISP1.

So sichern Sie die Datenebene an der Domänengrenze inhibit (*,G) joins durch Filter gegen "host 0.0.0.0" und administrativ abgegrenzte Adressen mithilfe des Befehls **multicast border**:

Abb. 13: Domänenübergreifende (*,G) Filter

```
ip access-list extended interdomain-sm-edge
  deny   ip  host 0.0.0.0 any
  deny   ip  any          239.0.0.0 0.255.255.255
  permit ip  any          any

Interface ethernet 0
  ip multicast boundary interdomain-sm-edge out
  ip multicast boundary interdomain-sm-edge in
```

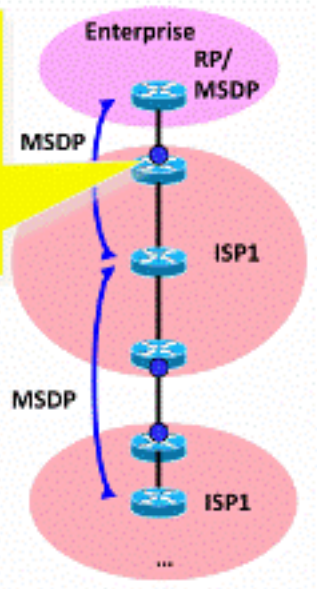

Abb. 13_Interdomain_Filter

Zur Sicherung der Kontrollebene muss die MSDP mithilfe von drei grundlegenden Sicherheitsmaßnahmen gehärtet werden:

1) MSDP-SA-Filter

Es ist eine "bewährte Vorgehensweise", den Inhalt von MSDP-Nachrichten über MSDP-SA-Filter

zu filtern. Die Grundidee dieses Filters besteht darin, die Weitergabe des Multicast-Zustands für Anwendungen und Gruppen zu vermeiden, die keine Internetanwendungen sind und nicht über die Quelldomäne hinaus weitergeleitet werden müssen. Im Idealfall lassen die Filter aus Sicherheitsgründen nur bekannte Gruppen (und möglicherweise Absender) zu und lehnen unbekannte Absender und/oder Gruppen ab.

Es ist in der Regel nicht möglich, alle zulässigen Absender und/oder Gruppen explizit aufzulisten. Es wird empfohlen, den Standardkonfigurationsfilter für PIM-SM-Domänen mit einem einzigen RP für jede Gruppe (keine MSDP-Mesh-Gruppe) zu verwenden:

```
!--- 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 !
```

Es wird empfohlen, die Filter so streng wie möglich und in beide Richtungen, eingehend und ausgehend, zu gestalten.

Weitere Informationen zu den Filterempfehlungen für MSDP-SA finden Sie unter: https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) MSDP-Zustandsbeschränkung

Wenn MSDP zwischen mehreren autonomen Systemen (AS) aktiviert ist, wird empfohlen, den im Router integrierten Status aufgrund von "Source-Active" (SA)-Nachrichten zu begrenzen, die von Nachbarn empfangen werden. Sie können den Befehl **ip msdp sa-limit** verwenden:

ip msdp sa-limit <peer> <limit>

Abb. 14: MSDP-Kontrollebene

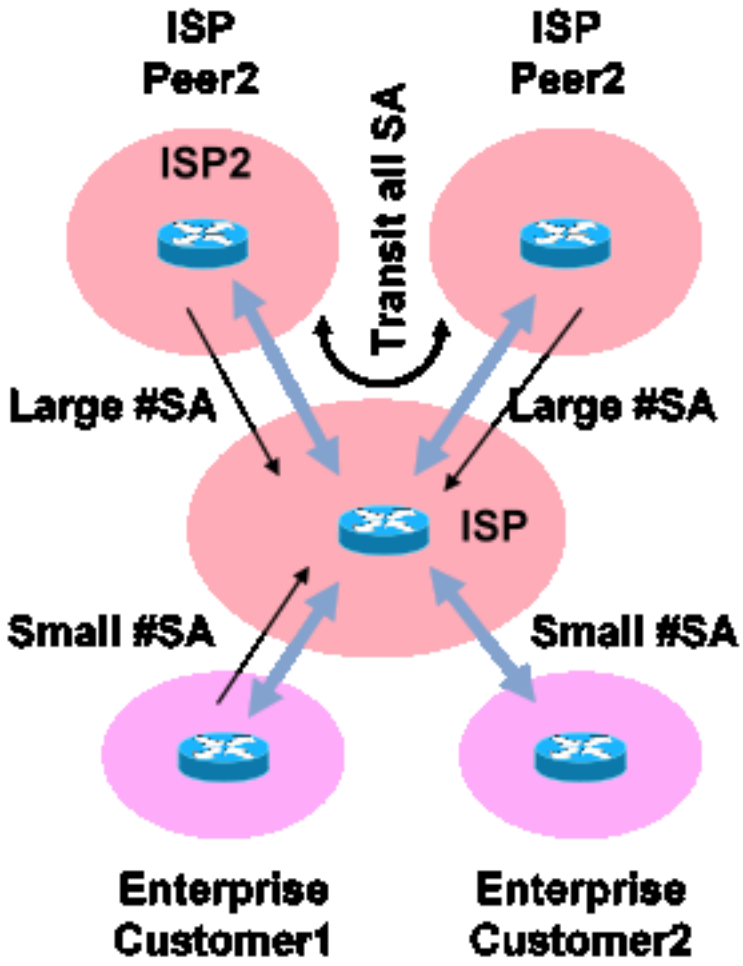

Abb. 14_MSDP_Kontrollebene

Mit dem Befehl **ip msdp sa-limit** können Sie die Anzahl der SA-Zustände begrenzen, die aufgrund von SA-Nachrichten erstellt werden, die von einem MSDP-Peer akzeptiert werden. Hier einige einfache Empfehlungen:

- Kleiner Grenzwert von Stub-Neighbor
- Großer Grenzwert für Transit-Nachbar (z. B. Höchstwert #SAs im Internet)
- Transit-ISP: Konfigurieren Sie das maximale #SAs, das Ihre Plattform unterstützen kann.

3) Nachbar-Authentifizierung mit MSDP MD5

Es wird empfohlen, die Passwortauthentifizierung mittels Message-Digest Algorithm (MD5) auf MSDP-Peers anzuwenden. Dabei wird die Option für die TCP MD5-Signatur verwendet. Dies entspricht der in RFC 6691 beschriebenen Verwendung zum Sichern von BGP.

Abb. 15: Nachbar-Authentifizierung mit MSDP MD5

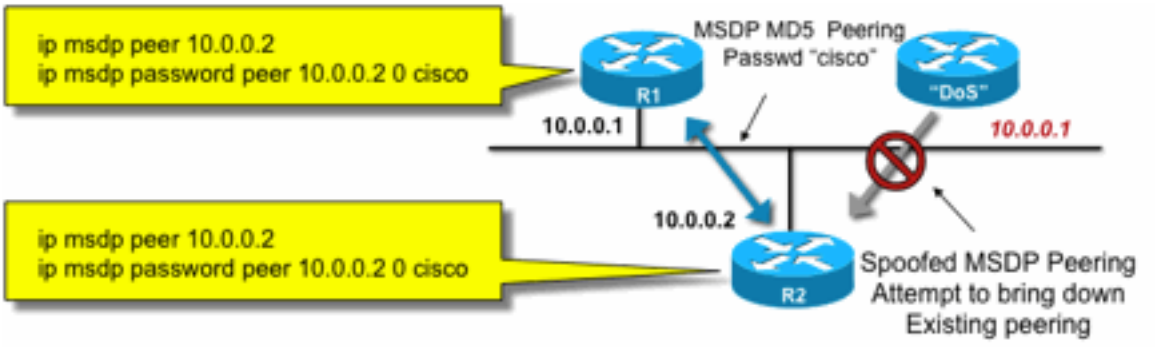

Abb. 15_MSDP_MD5Auth

Diese drei MSDP-Sicherheitsempfehlungen verfolgen unterschiedliche Ziele:

- Die Nachbarauthentifizierung (mit MD5) stellt sicher, dass nur vertrauenswürdige MSDP-Peers Nachrichten senden können.
- Die SA-Filter stellen sicher, dass selbst ein vertrauenswürdiger MSDP-Peer nur SA-Ankündigungen senden kann, die mit einer zuvor vereinbarten Quell-/Gruppenrichtlinie im Einklang stehen.
- Der SA-Grenzwert stellt außerdem sicher, dass der verfügbare Speicher selbst bei legitimen (S,G) Ankündigungen von legitimen Peers nicht ausgeschöpft werden kann.

Absender-/Quellprobleme

Viele Multicast-Sicherheitsprobleme, die vom Absender ausgehen, können durch geeignete Unicast-Sicherheitsmechanismen behoben werden. Eine Reihe von Unicast-Sicherheitsmechanismen werden hier als Best Practices empfohlen:

- **Spoofschutz für Quelladressen** (Unicast Reverse Path Forwarding, uRPF oder ACL und IP Source Guard für den Access Layer)
- **Infrastruktur-ACLs** (deny ip any (to) <Core-Adressraum>)

Solche Maßnahmen können dazu verwendet werden, gezielte Angriffe auf den Kern zu blockieren. Auf diese Weise können beispielsweise auch Probleme wie Angriffe gelöst werden, bei denen PIM-Unicast-Pakete an den RP gesendet werden, der sich "innerhalb" des Netzwerks befindet und daher durch die Infrastruktur-ACL geschützt ist.

Paketfilter-basierte Zugriffskontrolle - Steuerungsquellen

Im Beispiel in Abbildung 16 wird der Filter an der LAN-Schnittstelle (E0) des First-Hop-Multicast-Routers (Designated Router) konfiguriert. Der Filter wird durch eine erweiterte Zugriffskontrollliste mit der Bezeichnung "source" definiert. Diese ACL wird auf die an die Quelle gerichtete Schnittstelle des designierten Routers angewendet, der mit dem Quell-LAN verbunden ist. Aufgrund der Art des Multicast-Datenverkehrs kann ein ähnlicher Filter für alle LAN-Schnittstellen konfiguriert werden, auf denen Quellen aktiv werden können. Da es nicht in allen Fällen möglich ist, genau zu wissen, wo die Quellaktivität auftritt, wird empfohlen, solche Filter auf alle Eingangspunkte im Netzwerk anzuwenden.

Abb. 16: Kontrollquellen

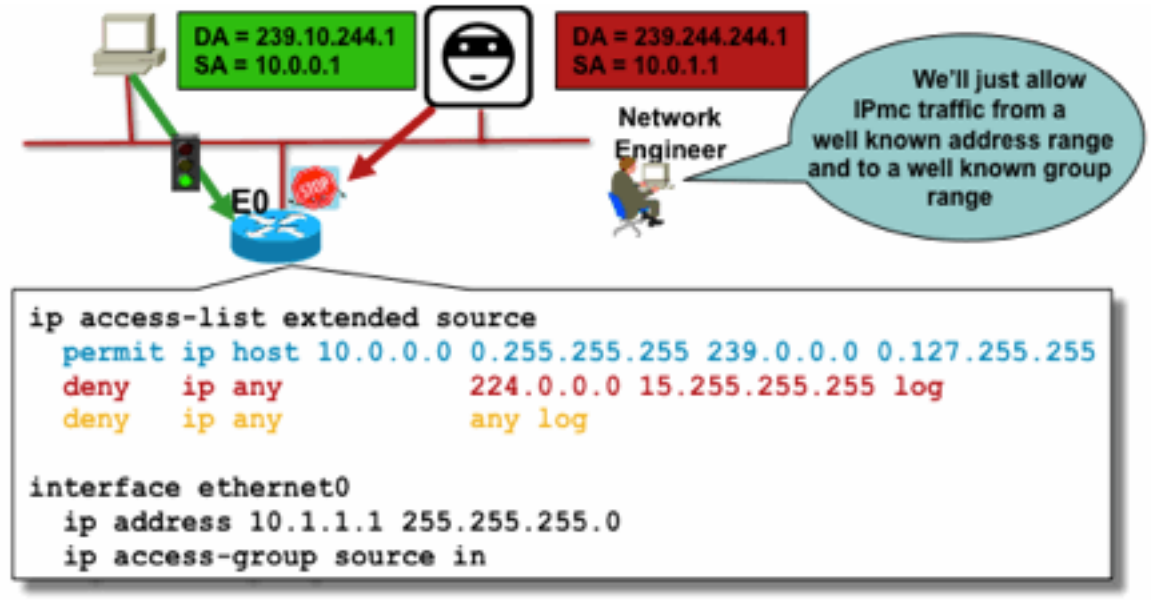

Abb. 16_Controlling_Sources

Der Zweck dieses Filters besteht darin, Datenverkehr von einer bestimmten Quelle oder einem bestimmten Bereich von Quelladressen zu einer bestimmten Gruppe oder einem bestimmten Bereich von Gruppenadressen zu verhindern. Dieser Filter wird verwendet, bevor PIM Mroute erstellt, und hilft, den Status zu begrenzen.

Dies ist eine standardmäßige Datenebenen-ACL. Dies wird auf ASICs auf High-End-Plattformen implementiert, und es treten keine Leistungseinbußen auf. ACLs auf Datenebene werden für direkt verbundene Quellen empfohlen und gegenüber der Steuerungsebene bevorzugt, da sie die Auswirkungen auf die Steuerungsebene durch unerwünschten Datenverkehr minimieren. Außerdem ist es sehr effektiv, das Ziel (IP-Multicast-Gruppenadressen) zu begrenzen, an das Pakete gesendet werden können. Da es sich hierbei um einen Router-Befehl handelt, kann eine gefälschte Quell-IP-Adresse nicht überwunden werden (siehe voriger Teil dieses Abschnitts). Daher wird empfohlen, entweder zusätzliche Layer-2-Mechanismen (L2) oder eine konsistente Richtlinie für alle Geräte bereitzustellen, die eine Verbindung zu einem bestimmten lokalen Netzwerk/virtuellen lokalen Netzwerk (LAN/VLAN) herstellen können.

> **Anmerkung:** Das Schlüsselwort "log" in einer ACL ist sehr nützlich, um Treffer für einen bestimmten ACL-Eintrag zu verstehen. Dies beansprucht jedoch CPU-Ressourcen und muss mit Vorsicht behandelt werden. Außerdem werden auf hardwarebasierten Plattformen ACL-Protokollmeldungen von einer CPU generiert, sodass die Auswirkungen auf die CPU berücksichtigt werden müssen.

PIM-SM-Quellcodeverwaltung

Einer der tatsächlichen Vorteile der ASM/PIM-SM-Architektur im Hinblick auf die Sicherheit ist die Tatsache, dass der Rendezvous Point einen einzigen Kontrollpunkt für alle Quellen im Netzwerk für jeden Gruppenbereich bietet. Dies kann mit einem Gerät namens Akzeptieren-Registrieren-Filter genutzt werden. Der Befehl für diesen Filter lautet wie folgt:

ip pim accept-register / ipv6 pim accept-register

Abb. 17: PIM-SM-Quellcodeverwaltung

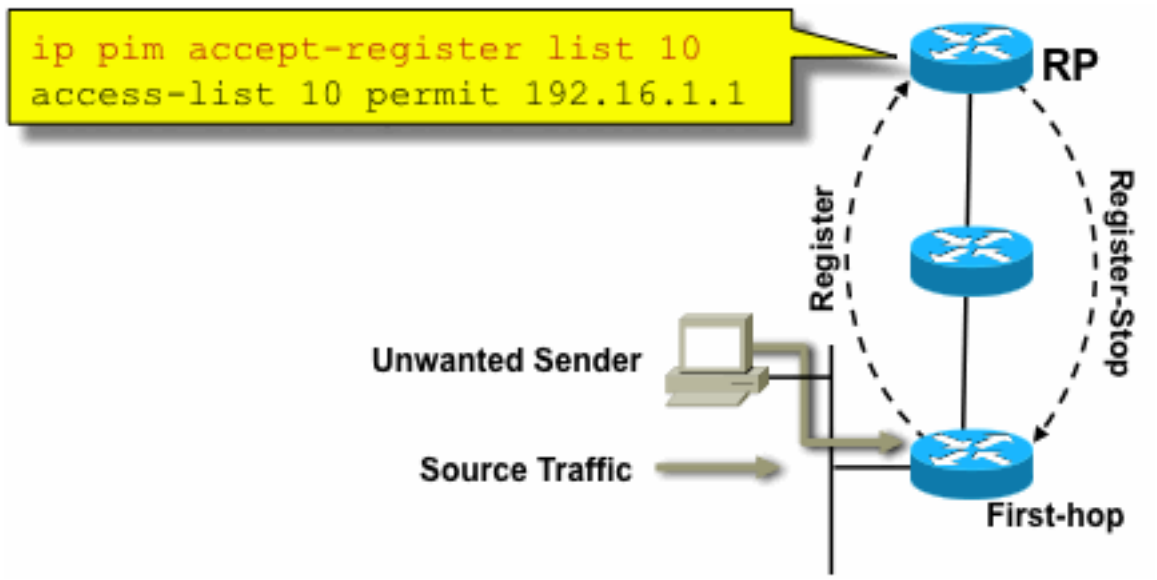

Abb. 17_PIMSM_Control

In einem PIM-SM-Netzwerk kann mit diesem Befehl eine Quelle für unerwünschten Datenverkehr gesteuert werden. Wenn der Quelldatenverkehr den First-Hop-Router erreicht, erstellt der First-Hop-Router (DR) den Status (S,G) und sendet eine PIM Source Register-Nachricht an den RP. Wenn die Quelle nicht in der Liste der Accept-Register-Filter (konfiguriert auf dem RP) aufgeführt ist, lehnt der RP die Registrierung ab und sendet eine sofortige Register-Stopp-Nachricht an den DR zurück.

Im gezeigten Beispiel wurde eine einfache ACL auf den RP angewendet, die nur nach der Quelladresse filtert. Es ist auch möglich, die Quelle UND die Gruppe mithilfe einer erweiterten Zugriffskontrollliste auf dem RP zu filtern.

Es gibt Nachteile von Quellfiltern, da mit dem Befehl **pim accept-register** auf dem RP der Status von PIM-SM (S,G) auf dem First-Hop-Router der Quelle weiterhin erstellt wird. Dies kann zu Datenverkehr an Empfängern führen, die sich vor Ort zwischen der Quelle und dem RP befinden. Der Befehl **pim accept-register** funktioniert darüber hinaus auf der Kontrollebene des RP. Dies kann dazu verwendet werden, den RP mit gefälschten Registernachrichten zu überlasten und möglicherweise eine DoS-Bedingung zu verursachen.

Es wird empfohlen, den Befehl pim accept-register auf dem RP zusätzlich zu anderen Methoden anzuwenden, z. B. die Anwendung einfacher Datenebenen-ACLs auf allen DRs an allen Eingangspunkten im Netzwerk. Während Eingangs-ACLs auf dem DR in einem perfekt konfigurierten und betriebenen Netzwerk ausreichen würden, wird empfohlen, den Befehl **pim accept-register** auf dem RP als sekundären Sicherheitsmechanismus zu konfigurieren. Fehlkonfigurationen auf den Edge-Routern. Mehrschichtige Sicherheitsmechanismen mit demselben Ziel werden als "tief greifende Abwehr" bezeichnet und gelten als gemeinsames Designprinzip für die Sicherheit.

Empfängerprobleme - IGMP/MLD steuern

Die meisten Empfängerprobleme fallen in die Domäne der IGMP/MLD-

Empfängerprotokollinteraktionen.

Abb. 18: IGMP steuern

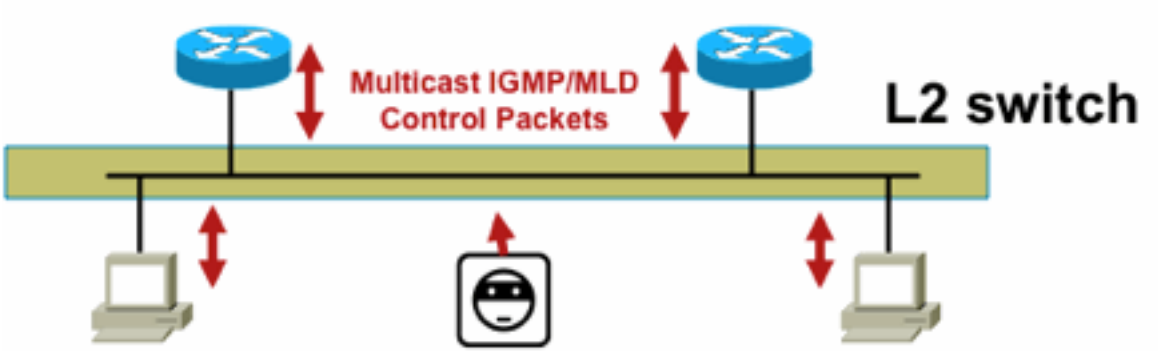

Abb. 18 - Controlling IGMP

Bei der Filterung von IGMP- oder MLD-Paketen sind folgende Punkte zu beachten:

- IPv4: IGMP ist ein IPv4-Protokolltyp (IPv4 Protokoll 2)
- IPv6: MLD wird in ICMPv6-Protokollpaketen übertragen

Der IGMP-Prozess wird standardmäßig aktiviert, sobald IP Multicast aktiviert ist. IGMP-Pakete enthalten auch diese Protokolle. Daher werden alle diese Protokolle bei Aktivierung von Multicast aktiviert:

- PIMv1 - PIMv1 war die erste Version von PIM und wird zu Migrationszwecken in Cisco IOS aktiviert. Bei aktuellen Bereitstellungen wird PIMv2 verwendet.
- Mrinfo - Mrinfo ist ein Unix-Befehl, den Cisco IOS zur Anzeige von Multicast-Nachbarn geerbt hat. Cisco empfiehlt die Verwendung von SNMP anstelle des Befehls mrinfo.
- DVMRP - DVMRP ist ein älteres Distanzvektorprotokoll im Dense-Modus mit sehr begrenzten Skalierungseigenschaften. Die Cisco IOS-Unterstützung für DVMRP wurde eingestellt oder ist bereits veraltet.
- Mtrace - Mtrace ist das Multicast-Äquivalent von Unicast-"Traceroute" und ein nützliches Tool.

Weitere Informationen finden Sie unter IGMP-Typnummern (Internet Group Management Protocol) der IANA

```
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
```

Unicast-IGMP-Pakete (für IGMP/UDLR) können gefiltert werden, da es sich dabei höchstwahrscheinlich um Angriffspakete und nicht um gültige IGMP-Protokollpakete handelt. Unicast-IGMP-Pakete werden von Cisco IOS zur Unterstützung unidirektionaler Verbindungen und anderer Ausnahmebedingungen unterstützt.

Gefälschte IGMP/MLD-Abfragepakete können zu einer niedrigeren IGMP-Version führen als erwartet.

Insbesondere senden Hosts idealerweise niemals IGMP-Abfragen, da eine mit einer niedrigeren IGMP-Version gesendete Abfrage dazu führen kann, dass alle Hosts, die diese Abfrage empfangen, auf die niedrigere Version zurückgesetzt werden. Bei Vorhandensein von IGMPv3/SSM-Hosts können die SSM-Streams "angegriffen" werden. Bei IGMPv2 kann dies zu längeren Wartezeiten führen.

Wenn ein nicht redundantes LAN mit einer einzigen IGMP-Abfrage vorhanden ist, muss der Router empfangene IGMP-Abfragen verwerfen.

Wenn ein redundantes/gemeinsames passives LAN vorhanden ist, ist ein Switch erforderlich, der IGMP-Snooping unterstützen kann. In diesem Fall können zwei spezifische Funktionen hilfreich sein:

- Router Guard
- IGMP-Mindestversion - Befehl

Router Guard

Jeder Switch-Port kann ein Multicast-Router-Port werden, wenn der Switch an diesem Port ein Multicast-Router-Steuerungspaket (IGMP General Query, PIM Hello oder CGMP Hello) empfängt. Wenn ein Switch-Port zu einem Multicast-Router-Port wird, wird der gesamte Multicast-Datenverkehr an diesen Port gesendet. Dies kann mit "Router Guard" verhindert werden. Für die Router Guard-Funktion muss IGMP-Snooping nicht aktiviert sein.

Mit der Router Guard-Funktion kann ein bestimmter Port als Multicast-Host-Port festgelegt werden. Der Port kann kein Router-Port werden, selbst wenn Multicast-Router-Steuerungspakete empfangen werden.

Diese Pakettypen werden verworfen, wenn sie an einem Port mit aktiviertem Router Guard empfangen werden:

- IGMP-Abfragenachrichten
- IPv4-PIMv2-Nachrichten
- IGMP-PIM-Nachrichten (PIMv1)
- IGMP-DVMRP-Nachrichten
- Router-Port Group Management Protocol (RGMP)-Nachrichten
- Cisco Group Management Protocol (CGMP)-Nachrichten

Wenn diese Pakete verworfen werden, werden Statistiken aktualisiert, die anzeigen, dass Pakete aufgrund von Router Guard verworfen werden.

IGMP-Mindestversion

Es ist möglich, die zulässige Mindestversion der IGMP-Hosts zu konfigurieren. Sie können beispielsweise alle IGMPv1-Hosts oder alle IGMPv1- und IGMPv2-Hosts deaktivieren. Dieser Filter gilt nur für Mitgliedsberichte.

Wenn die Hosts an ein gemeinsames "passives" LAN angeschlossen sind (z. B. an einen Switch, der IGMP-Snooping nicht unterstützt oder dafür nicht konfiguriert ist), kann ein Router solche falschen Abfragen auch nicht bearbeiten, außer die Mitgliedsberichte der "alten Version" zu ignorieren, die dann ausgelöst werden und nicht auf sich selbst zurückgreifen.

Da IGMP-Abfragen für alle Hosts sichtbar sein müssen, ist es nicht möglich, Hash-basierte Nachrichtenauthentifizierungsmechanismen (HMAC) mit einem Pre-Shared Key, z. B. dem statischen Schlüssel IPSec, zur Authentifizierung von IGMP-Abfragen von "gültigen Routern" zu verwenden. Wenn zwei oder mehr Router mit einem gemeinsamen LAN-Segment verbunden sind, muss der IGMP-Abfrager ausgewählt werden. In diesem Fall kann als einziges Filter ein IP-Zugriffsgruppenfilter verwendet werden, der auf der Quell-IP-Adresse des anderen IGMP-Routers basiert, der Abfragen sendet.

"Normale" Multicast-IGMP-Pakete müssen zugelassen werden.

Dieser Filter kann an Empfänger-Ports verwendet werden, um nur "gute" IGMP-Pakete zuzulassen und um bekannte "schlechte" zu filtern:

```
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
```

> **Anmerkung:** Dieser IGMP-Filtertyp kann in Empfangs-ACLs oder CoPP verwendet werden. In beiden Anwendungen muss sie mit Filtern für anderen verarbeiteten Datenverkehr kombiniert werden, z. B. Routing- und Verwaltungsebenenprotokolle.

Abb. 19: Host Receiver-seitige Zugriffskontrolle

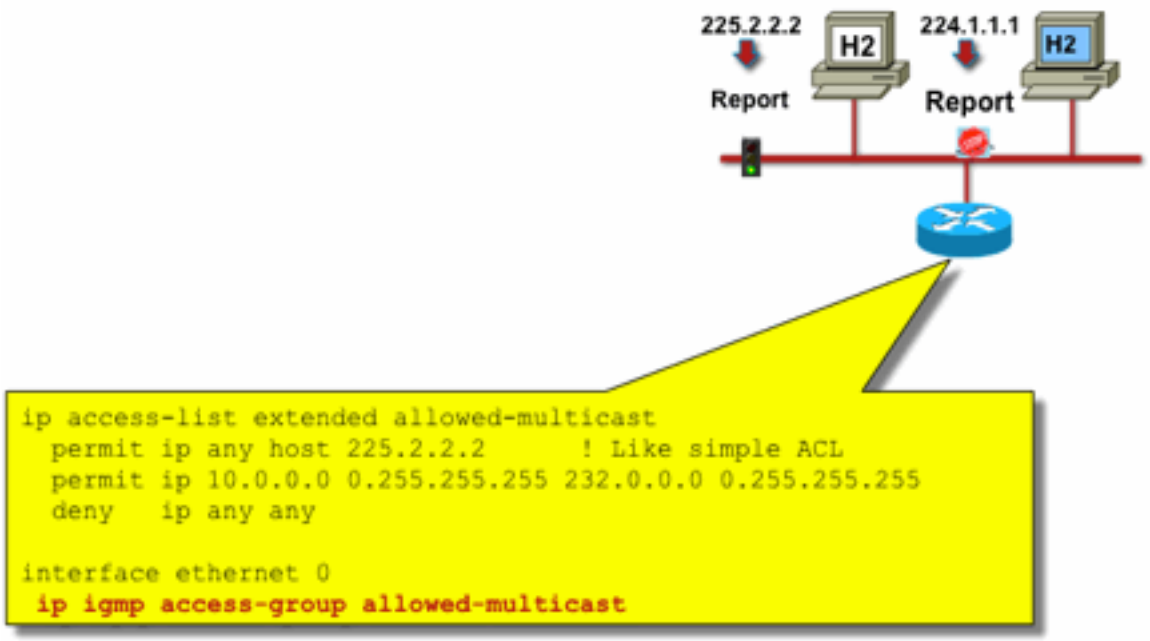

Abb.

Zum Filtern des Datenverkehrs zu einem Empfänger muss nicht der Datenverkehr der Datenebene gefiltert werden, sondern das IGMP-Protokoll der Kontrollebene. Da IGMP eine erforderliche Voraussetzung für den Empfang von Multicast-Datenverkehr ist, sind keine Filter auf Datenebene erforderlich.

Sie können insbesondere festlegen, welchen Multicast-Flows Empfänger beitreten können (verbunden mit der Schnittstelle, für die der Befehl konfiguriert wurde). Verwenden Sie in diesem Fall den Befehl **ip igmp access-group / ipv6 mld access-group**:

```
ip igmp access-group / ipv6 mld access-group
```

Bei ASM-Gruppen wird mit diesem Befehl nur nach der Zieladresse gefiltert. Die Quell-IP-Adresse in der ACL wird dann ignoriert. Bei SSM-Gruppen, die IGMPv3/MLDv2 verwenden, werden die Quell- und Ziel-IP-Adressen gefiltert.

In diesem Beispiel wird eine bestimmte Gruppe für alle IGMP-Router gefiltert:

```
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
```

In diesem Beispiel werden bestimmte IGMP-Lautsprecher (also bestimmte Multicast-Empfänger) für eine bestimmte Gruppe gefiltert:

```
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
```

> **Anmerkung:** Bei ASM-Gruppen wird die Quelle ignoriert.

Zugangskontrolle

Die Zugriffskontrolle gibt für bestimmte Datenflüsse eine binäre Antwort mit "Ja" oder "Nein" aus, unabhängig vom Status des Netzwerks. Die Zugangskontrolle dagegen schränkt die Anzahl der Ressourcen ein, die ein Sender/Empfänger nutzen kann, vorausgesetzt, sie haben die Zugriffskontrollmechanismen bestanden. Für die Zugangskontrolle in einer Multicast-Umgebung stehen verschiedene Geräte zur Verfügung.

IGMP-Grenzwerte global und pro Schnittstelle

Auf dem Router, der interessierten Multicast-Empfängern am nächsten ist, besteht die Möglichkeit, die Anzahl der IGMP-Gruppen zu begrenzen, die sowohl global als auch pro Schnittstelle hinzugefügt werden. Sie können die Befehle **ip igmp limit/ipv6 mld limit** verwenden:

```
ip igmp limit <n> [ except <ext-acl> ]
ipv6 mld limit <n> [ except <ext-acl> ]
```

Es wird empfohlen, diese Grenze immer pro Schnittstelle und global zu konfigurieren. In jedem Fall bezieht sich der Grenzwert auf die Anzahl der Einträge im IGMP-Cache.

Die nächsten beiden Beispiele zeigen, wie dieser Befehl verwendet werden kann, um die Anzahl der Gruppen am Edge eines Breitbandnetzwerks zu begrenzen.

Beispiel 1: Beschränkung der empfangenen Gruppen auf SDR-Ankündigungen und einen empfangenen Kanal

Das Sitzungsverzeichnis (Session Directory, SDR) dient als Kanalführung für einige Multicast-Empfänger. Weitere Informationen finden Sie unter RFC 2327.

Eine allgemeine Anforderung besteht darin, die Empfänger auf den Empfang der SD-Gruppe und eines Kanals zu beschränken. Diese Beispielkonfiguration kann verwendet werden:

```
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
```

Die Zugriffsliste in diesem Beispiel gibt nur die Kanalführung an. Mit dem globalen Befehl **ip igmp limit** wird jede IGMP-Quelle auf einen einzelnen (1) Kanal beschränkt. Der Channel Guide, der immer empfangen werden kann, ist jedoch nicht enthalten. Der Schnittstellenbefehl überschreibt den globalen Befehl und ermöglicht den Empfang von zwei (2) Kanälen zusätzlich zum Kanalführer auf dieser Schnittstelle.

Beispiel 2 - Zugangskontrolle auf der Aggregation-DSLAM-Verbindung

Dieser Befehl kann auch verwendet werden, um eine Form der Bandbreitenzugangssteuerung bereitzustellen. Wenn beispielsweise 300 SDTV-Kanäle mit jeweils 4 Mbit/s verteilt werden müssen und eine 1-Gbit/s-Verbindung zum Digital-Subscriber-Line-Access-Multiplexer (DSLAM) besteht, können Sie eine Richtlinienentscheidung treffen, die TV-Bandbreite auf 500 Mbit/s zu begrenzen und den Rest für Internet- und andere Zwecke zu belassen. In diesem Fall können Sie die IGMP-Status auf 500 Mbit/s/4 Mbit/s = 125 IGMP-Status begrenzen.

Diese Konfiguration kann in folgenden Fällen verwendet werden:

Abb. 20: Verwendung von IGMP-Grenzwerten pro Schnittstelle; Zugangskontrolle auf Agg-DSLAM-Verbindung

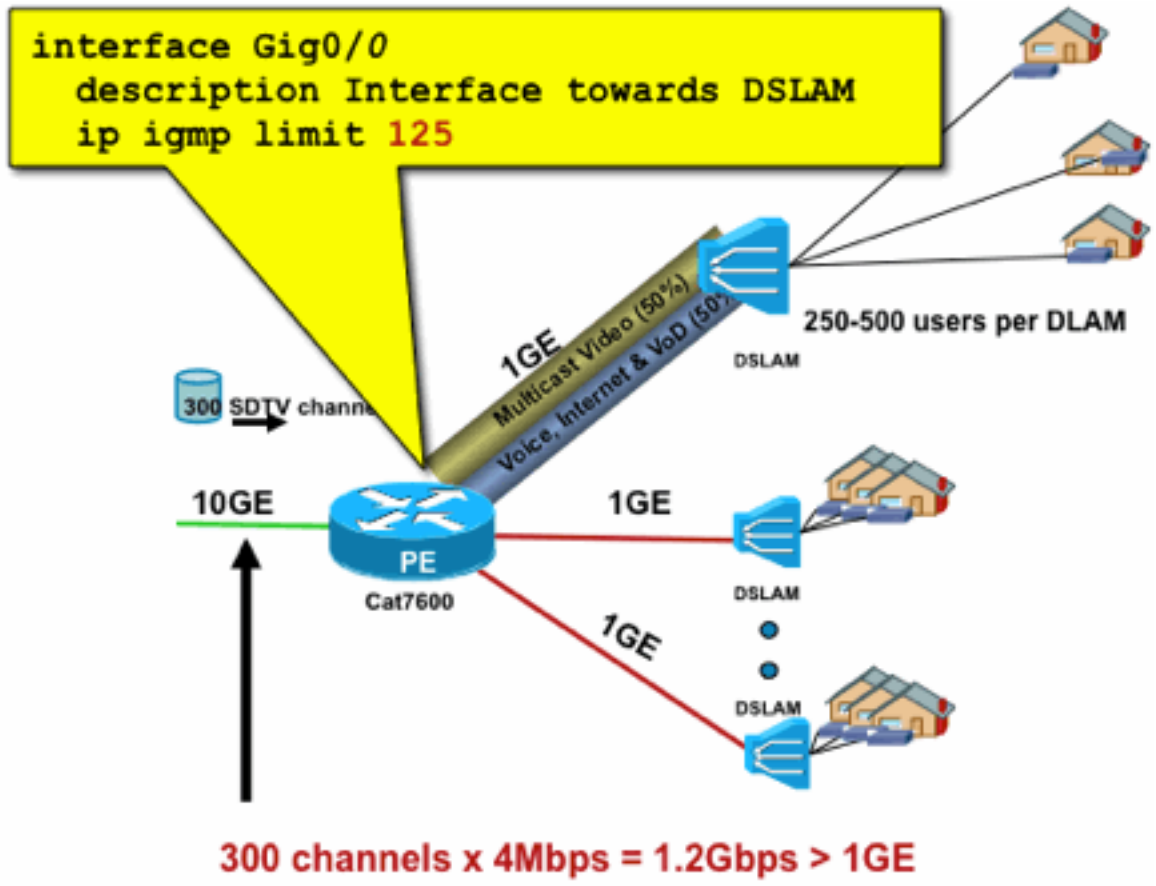

Abb. 20_PerInterface_IGMP

Schnittstellenspezifische Routengrenzwerte

Die Aktivierung von schnittstellenspezifischen mroute-Statuslimits ist eine eher allgemeine Form der Zugangskontrolle. Sie schränkt nicht nur den IGMP- und PIM-Status einer ausgehenden Schnittstelle ein, sondern bietet auch eine Möglichkeit zur Festlegung von Statusgrenzen für eingehende Schnittstellen.

Verwenden Sie den Befehl **ip multicast limit**:

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

Der Status kann separat auf Eingangs- und Ausgangsschnittstellen beschränkt werden. Der direkt angeschlossene Quellstatus kann auch mithilfe des Schlüsselworts "connected" eingeschränkt werden. Beispiele für die Verwendung dieses Befehls:

Beispiel 1: Zugangskontrolle am Ausgang der Agg-DSLAM-Verbindung

In diesem Beispiel gibt es 300 SD-TV-Kanäle. Es wird angenommen, dass jeder SD-Kanal 4 Mbit/s benötigt, mit einer Gesamtzahl von maximal 500 Mbit/s. Gehen Sie außerdem davon aus, dass Support-Pakete für Basic, Extended und Premium erforderlich sind. Beispiel für Bandbreitenzuweisungen:

- 60 % (300 Mbit/s Basic)
- 20 %/100 Mbit/s erweitert
- 20 % / 100 Mbit/s Premium

Verwenden Sie dann 4 Mbit/s pro Kanal, beschränken Sie den DSLAM-Uplink auf:

- Grundlegende 75 Status
- Erweitert auf 25 Staaten
- Premium 25 Staaten

Konfigurieren Sie den Grenzwert für die ausgehende Schnittstelle, die dem DSLAM aus dem PEAgg gegenüberliegt:

Abb. 21: Verwendung von Schnittstellenspezifischen Routengrenzwerten; Zugangskontrolle auf Agg-DSLAM-Verbindung

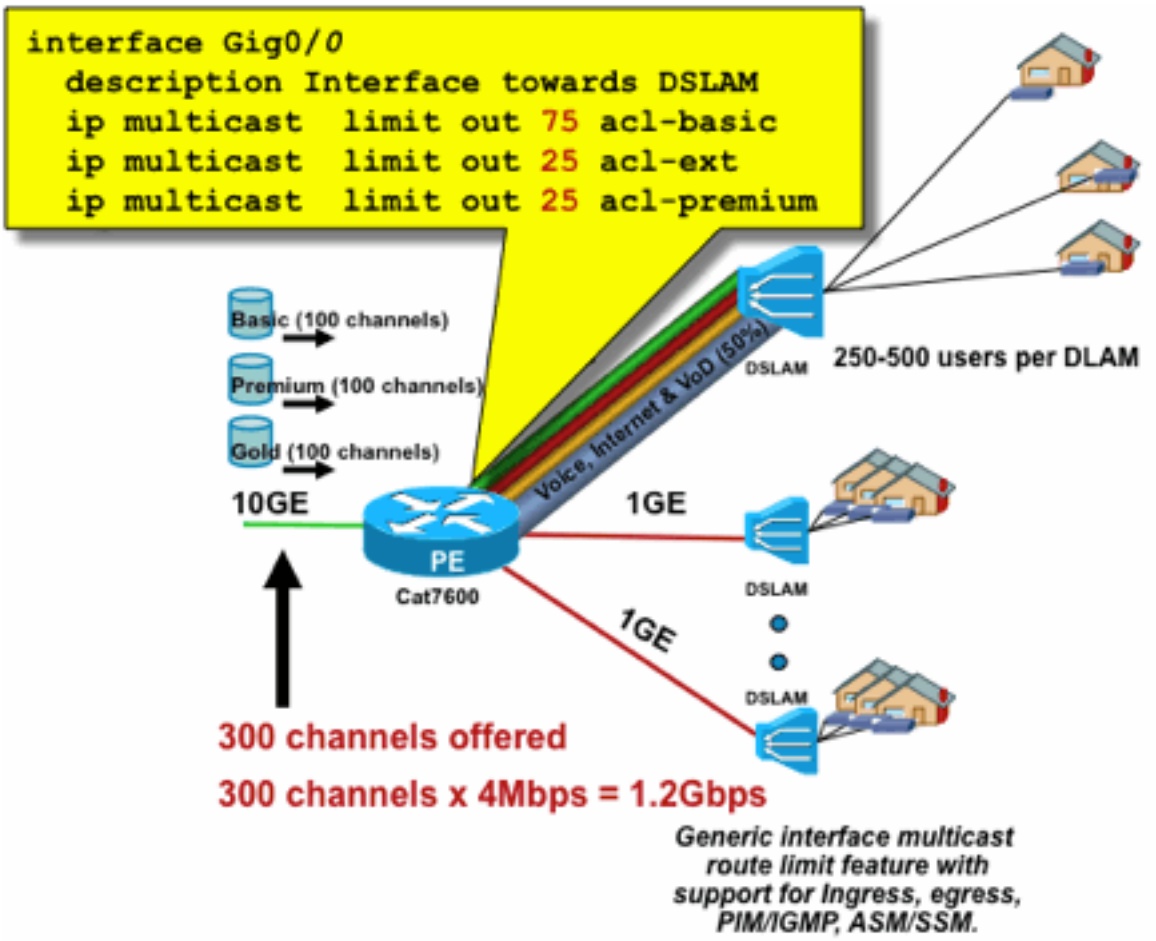

Abb. 21_PerInterface_Mroute

Beispiel 2 - Zugangskontrolle bei Eingang auf Agg-DSLAM-Verbindung

Statt des "Out"-Limits für die ausgehende Schnittstelle des Upstream-Geräts können RPF-Limits für die RPF-Schnittstelle des Downstream-Geräts verwendet werden. Dies hat im Grunde das gleiche Ergebnis wie im vorherigen Beispiel und könnte nützlich sein, wenn das Downstream-Gerät kein Cisco IOS-Gerät ist.

Abb. 22: Verwendung von Schnittstellenspezifischen Routengrenzwerten; Zugangskontrolle für Eingabe

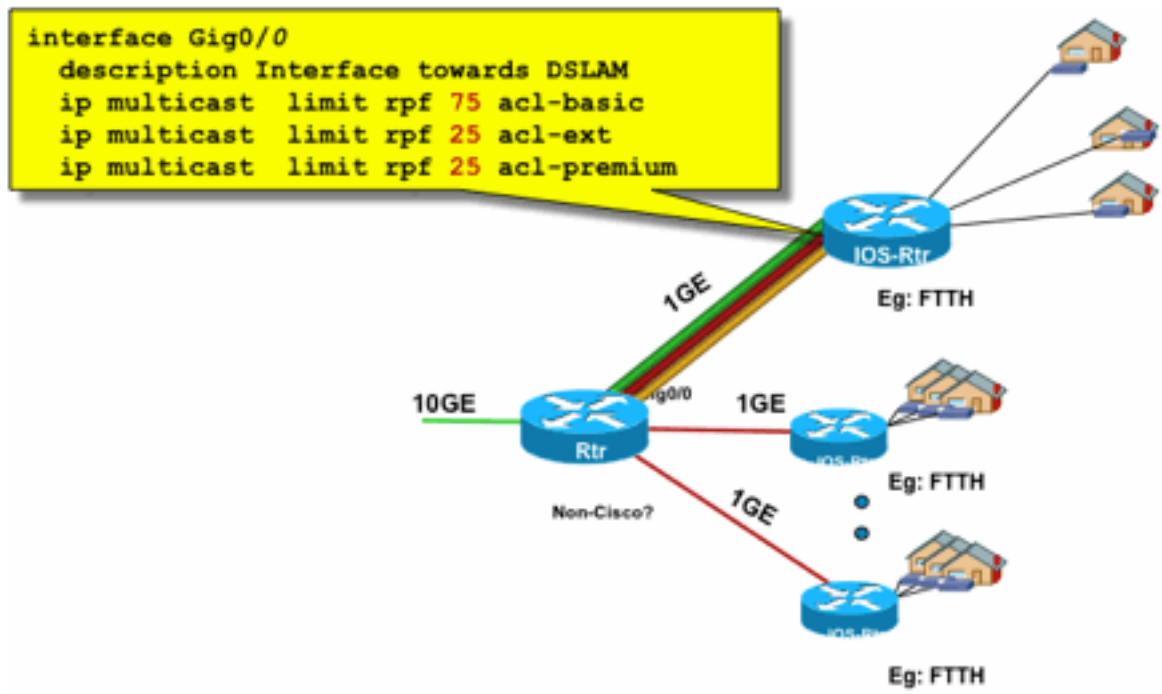

Abb. 22_PerInterface_Mroute_inputControl

Beispiel 3 - Bandbreitenbasierte Beschränkungen

Sie können eine weitere Unterteilung der Zugangsbandbreite zwischen mehreren Inhaltsanbietern vornehmen und jedem Inhaltsanbieter einen fairen Anteil der Bandbreite am Uplink zum DSLAM anbieten. Verwenden Sie in diesem Fall den **Befehl ip multicast limit cost**:

ip multicast limit cost <ext-acl> <multiplier>

Mit diesem Befehl kann ein "cost" (der unter "multiplier" angegebene Wert) jedem Status zugewiesen werden, der mit der erweiterten ACL im Grenzwert für IP-Multicast übereinstimmt.

Bei diesem Befehl handelt es sich um einen globalen Befehl, für den mehrere gleichzeitige Kosten konfiguriert werden können.

In diesem Beispiel ist es notwendig, drei verschiedene Content-Provider mit fairem Zugang zu jedem Netzwerk zu unterstützen. Außerdem müssen in diesem Beispiel MPEG-Streams (Moving Picture Experts Group) verschiedener Typen unterstützt werden:

MPEG2 SDTV: 4 Mbit/s
MPEG2-HDTV: 18 Mbit/s
MPEG4-SDTV: 1,6 Mbit/s
MPEG4-HDTV: 6 Mbit/s

In diesem Fall können Sie Bandbreitenkosten auf jeden Streamtyp aufteilen und den Rest der 750 Mbit/s auf die drei Inhaltsanbieter mit dieser Konfiguration aufteilen:

```
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
```

Abb. 23: Kostenfaktor für schnittstellenspezifische Mroute-Zustandsgrenzwerte

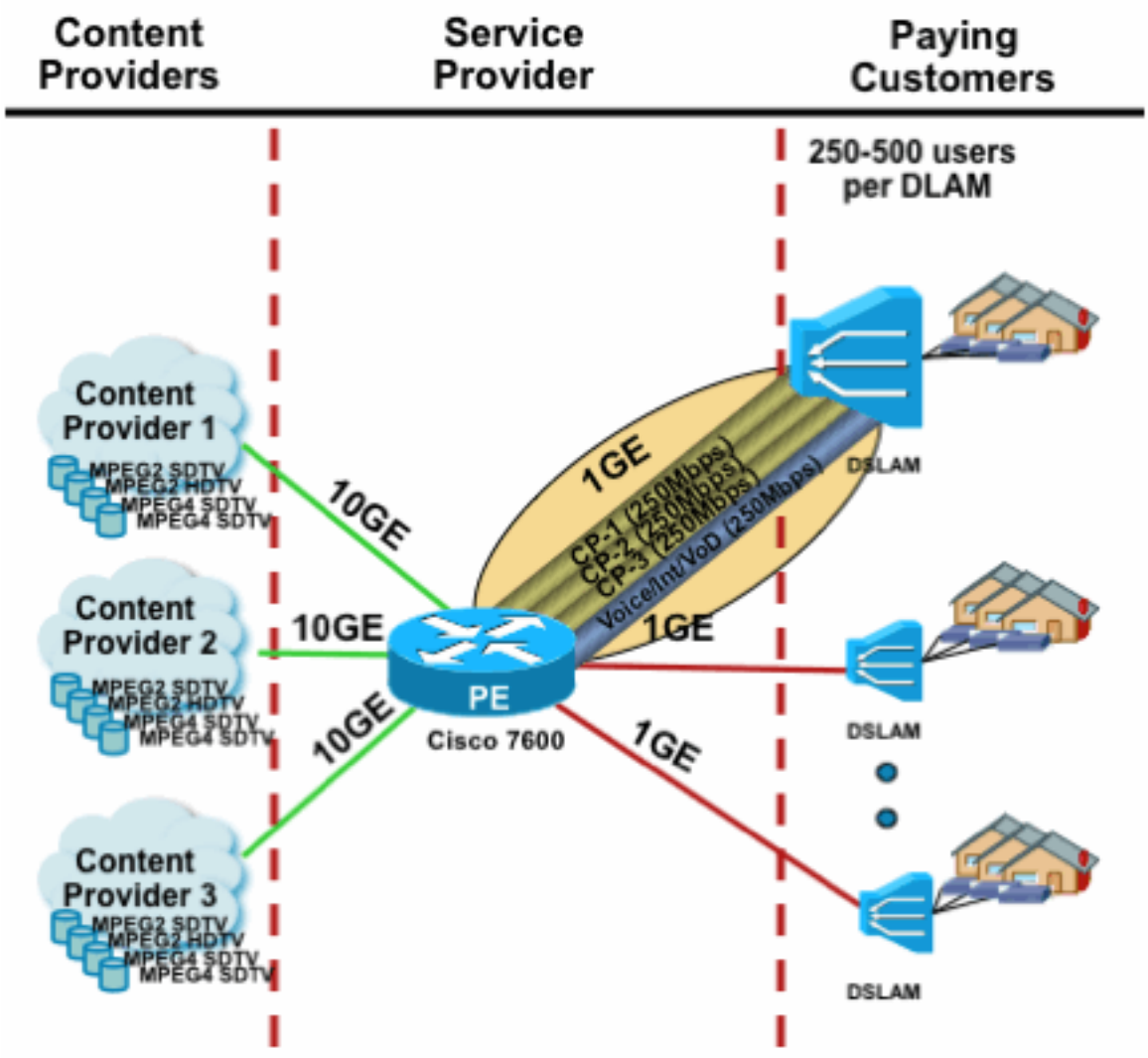

Abb. 23

Kosten pro Schnittstelle

Multicast und IPSec

Einführung in GET VPN

Wie bei Unicast muss auch Multicast-Datenverkehr manchmal gesichert werden, um Vertraulichkeit und Integrität zu gewährleisten. In zwei Hauptbereichen könnten solche Dienste erforderlich sein:

- Verschlüsselung von Multicast-Streams (z. B. in Banking-Anwendungen, die vertrauliche Daten an eine große Gruppe von Empfängern streamen, die Multicast verwenden) - das ist die Sicherheit der Datenebene.
- Verschlüsselung von Kontrollebenenprotokollen, die z. B. Multicast, OSPF oder PIM verwenden - dies ist die Sicherheit der Kontrollebene.

IPSec als Protokoll [RFCs 6040, 7619, 4302, 4303, 5282] ist speziell auf Unicast-Datenverkehr

(durch RFC) beschränkt. Dort wird eine "Sicherheitszuordnung" (Security Association, SA) zwischen zwei Unicast-Peers eingerichtet. Um IPSec auf Multicast-Datenverkehr anzuwenden, besteht eine Option darin, Multicast-Datenverkehr in einen GRE-Tunnel zu kapseln und IPSec anschließend auf den GRE-Tunnel (Unicast) anzuwenden. Bei einem neueren Ansatz wird eine einzige Sicherheitszuordnung verwendet, die zwischen allen Mitgliedern der Gruppe erstellt wird. Der Group Domain of Interpretation (GDOI) [RFC 6407] definiert, wie dies erreicht wird.

Auf der Grundlage von GDOI entwickelte Cisco eine Technologie mit dem Namen Group Encryption Transport (GET) VPN. Diese Technologie verwendet "Tunnel Mode with Address Preservation", wie im Dokument "draft-ietf-msec-ipsec-extensions" definiert. In GET VPN wird zunächst eine Gruppensicherheitszuordnung zwischen allen Mitgliedern der Gruppe erstellt. Anschließend wird der Datenverkehr entweder mit ESP (Encapsulated Security Payload) oder AH (Authentication Header) geschützt, der den Tunnelmodus mit Adressenerhaltung verwendet.

Zusammenfassend lässt sich sagen, dass GET-VPN ein Multicast-Paket kapselt, das die Adressinformationen des ursprünglichen Headers verwendet, und dann das innere Paket in Bezug auf die Gruppenrichtlinie schützt, beispielsweise mit einem ESP.

Der Vorteil von GET-VPN besteht darin, dass der Multicast-Datenverkehr durch die Mechanismen zur Sicherheitskapselung nicht beeinträchtigt wird. Die gerouteten IP-Header-Adressen bleiben dieselben wie der ursprüngliche IP-Header. Multicast-Datenverkehr kann auf die gleiche Weise mit oder ohne GET-VPN gesichert werden.

Die auf die GET-VPN-Knoten angewendete Richtlinie wird zentral auf einem Group Key-Server definiert und auf alle Gruppenknoten verteilt. Aus diesem Grund verfügen alle Gruppenknoten über die gleiche Richtlinie und die gleichen Sicherheitseinstellungen, die auf den Gruppenverkehr angewendet werden. Ähnlich wie beim Standard-IPSec definiert die Krypto-Richtlinie, welche Art von Datenverkehr auf welche Weise geschützt werden muss. Dadurch kann GET VPN für verschiedene Zwecke verwendet werden.

GET-VPN zur Verschlüsselung des Multicast-Datenverkehrs der Datenebene verwenden

Die netzwerkweite Verschlüsselungsrichtlinie wird auf dem Gruppenschlüsselserver festgelegt und an die GET-VPN-Endpunkte verteilt. Die Richtlinie enthält die IPSec-Richtlinie (IPSec-Modus - hier: Tunnelmodus mit Header-Erhaltung) und zu verwendende Sicherheitsalgorithmen (z. B. AES). Sie enthält außerdem eine Richtlinie, die beschreibt, welcher Datenverkehr gemäß der Definition einer ACL gesichert werden kann.

GET-VPN kann für Multicast- und Unicast-Datenverkehr verwendet werden. Eine Richtlinie zum Sichern von Unicast-Datenverkehr könnte durch eine ACL definiert werden:

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

Dies würde den gesamten Datenverkehr mit einer Quell-IP von 10/8 und einer Ziel-IP von 10/8 verschlüsseln. Der gesamte andere Datenverkehr, z. B. Datenverkehr von 10/8 an eine andere Adresse, würde vom GET-VPN ignoriert.

Die Anwendung von GET VPN für Multicast-Datenverkehr ist technisch identisch. Mit diesem Zugriffskontrolleintrag (Access Control Entry, ACE) kann beispielsweise der Datenverkehr von einer beliebigen Quelle zu den entsprechenden Multicast-Gruppen gesichert werden:

```
permit ip any 239.192.0.0 0.0.255.255
```

Diese Policy stimmt mit allen Quellen ("any") und allen Multicast-Gruppen überein, die mit 239.192 beginnen. Der Datenverkehr zu anderen Multicast-Gruppen ist nicht gesichert.

> **Anmerkung:** Große Aufmerksamkeit ist auf die Konstruktion der Crypto-ACL zu richten. Verwaltungsdatenverkehr oder Datenverkehr, der von außerhalb der GET-VPN-Domäne stammt, aber innerhalb dieser endet (d. h. Datenverkehr, der nur an einen Krypto-Endpunkt weitergeleitet wird), muss von der GDOI-Richtlinie ausgeschlossen werden.

Häufige Fehler sind:

- permit ip any 224.0.0.0 0.255.255.255: Dadurch wird auch OSPF- und anderer Steuerungsebenen-Datenverkehr verschlüsselt, der beispielsweise an einen Peer-Router gerichtet ist.
- Der Managementverkehr wird nicht aus der Krypto-Richtlinie ausgeschlossen, die innerhalb des Netzwerks endet. Dies schließt den GDOI-Datenverkehr selbst ein.

GET-VPN zur Authentifizierung des Datenverkehrs auf der Kontrollebene verwenden

Im Allgemeinen empfiehlt es sich, den Datenverkehr der Steuerungsebene wie Routing-Protokolle zu authentifizieren, um sicherzustellen, dass die Nachrichten von einem vertrauenswürdigen Peer stammen. Dies ist für Kontrollebenenprotokolle, die Unicast verwenden, wie BGP, vergleichsweise einfach. Viele Kontrollebenenprotokolle verwenden jedoch Multicast-Verkehr. Beispiele sind OSPF, RIP und PIM. Die vollständige Liste finden Sie in der IPv4 Multicast Address Space Registry der IANA.

Einige dieser Protokolle verfügen über integrierte Authentifizierungsfunktionen wie Routing Information Protocol (RIP) oder Enhanced Interior Group Routing Protocol (EIGRP). Andere verwenden IPSec, um diese Authentifizierung bereitzustellen (z. B. OSPFv3, PIM). Im letzteren Fall bietet GET VPN eine skalierbare Möglichkeit, diese Protokolle zu sichern. In den meisten Fällen ist die Protokollnachrichtenauthentifizierung erforderlich, d. h. die Überprüfung, ob eine Nachricht von einem vertrauenswürdigen Peer gesendet wurde. GET VPN ermöglicht jedoch auch die Verschlüsselung solcher Nachrichten.

Um diesen Steuerungsebenen-Datenverkehr zu sichern (in der Regel nur für die Authentifizierung), muss er mit einer ACL beschrieben und in die GET VPN-Richtlinie integriert werden. Die Details hängen vom zu sichernden Protokoll ab. Dabei muss berücksichtigt werden, ob die ACL Datenverkehr enthält, der nur über einen Eingangs-GET-VPN-Knoten (der gekapselt ist) oder einen Ausgangs-Knoten läuft.

Es gibt zwei grundlegende Möglichkeiten, PIM-Protokolle zu sichern:

- **permit ip any 224.0.0.13 0.0.0.0**: Dies ist die Multicast-Gruppe "Alle PIM-Router". Dies schützt jedoch keine Unicast-PIM-Nachrichten.
- **Erlauben Sie pim any**: Dadurch wird das PIM-Protokoll unabhängig davon gesichert, ob Multicast oder Unicast verwendet wird.

> **Anmerkung:** Die Befehle werden als Beispiele zur Erläuterung eines Konzepts angegeben. Beispielsweise müssen bestimmte PIM-Protokolle, die zum Bootstrap von PIM verwendet

werden, wie BSR oder Auto-RP ausgeschlossen werden. Neue Verfahren haben gewisse Vorteile und Unannehmlichkeiten, die von der Bereitstellung abhängen. Weitere Informationen zum Sichern von PIM mit GET VPN finden Sie in der entsprechenden Literatur.

Schlussfolgerungen

Multicast wird in Netzwerken immer häufiger verwendet. Das Aufkommen von IPTV-Diensten in Breitband-Heimnetzwerken und die Entwicklung hin zu elektronischen Handelsanwendungen auf vielen Finanzmärkten sind nur zwei Beispiele für Anforderungen, die Multicast zu einer absoluten Anforderung machen. Multicast bringt eine Vielzahl unterschiedlicher Herausforderungen in Bezug auf Konfiguration, Betrieb und Management mit sich. Eine der größten Herausforderungen ist die Sicherheit.

In diesem Dokument werden verschiedene Möglichkeiten zum Sichern von Multicast untersucht:

- Sehen Sie sich zunächst die gesamte Multicast-Kontroll- und Datenebene an, um zu erklären, wie die Unterschiede zu Unicast neue Sicherheitsherausforderungen darstellen.
- Anschließend wurden die wichtigsten Protokolle, die in einem Multicast-Netzwerk vorkommen, insbesondere IGMP, PIM und MSDP, eingehend untersucht. In jedem Fall wurden eine Beschreibung der Sicherheitsbedrohungen und empfohlene Best Practices zur Eindämmung dieser Bedrohungen bereitgestellt.
- Darüber hinaus gibt es einige Beispiele dafür, wie Multicast in bestimmten Anwendungen gesichert werden kann, z. B. in Breitband-Edge-Netzwerken, in denen die Bandbreite im Vergleich zur Bandbreite, die für bestimmte Videodatenströme erforderlich ist, begrenzt werden kann.
- Schließlich wurde die GET-VPN-Architektur als Mittel zur integrierten Multicast-Funktion mit IPSec für die Bereitstellung sicherer VPNs beschrieben.

Berücksichtigen Sie bei der Multicast-Sicherheit den Unterschied zu Unicast. Die Multicast-Übertragung basiert auf der Erstellung eines dynamischen Zustands, Multicast umfasst die dynamische Paketreplikation und Multicast erstellt unidirektionale Trees als Reaktion auf PIM JOIN/PRUNE-Nachrichten. Die Sicherheit dieser gesamten Umgebung erfordert das Verständnis und die Bereitstellung eines umfangreichen Frameworks von Cisco IOS-Befehlen. Diese Befehle konzentrieren sich hauptsächlich auf den Schutz von Protokollvorgängen, Zuständen (Multicast) oder Policern, die gegen Pakete wie CoPP gesetzt werden. Mit der richtigen Verwendung dieser Befehle ist es möglich, einen robusten geschützten Dienst für IP-Multicast bereitzustellen.

Zusammenfassend lässt sich sagen, dass in diesem Whitepaper verschiedene Ansätze beschrieben und gefördert werden:

1. Weit verbreitete Verwendung von SSM: Dies ist der einfachste PIM-Modus, der auch die Verwendung von (S,G)-Weiterleitung ermöglicht.
2. Wenn ASM-Services benötigt werden, stellen Sie sicher, dass ein zuverlässiger Service bereitgestellt werden kann. Die Verwendung statisch definierter RPs bietet eine sicherere Kontrollebene als dynamische RP-Ankündigungen. Auto-RP und BSR sind flexibler
3. Wenn PIM-SM aktiviert ist, prüfen Sie Bereiche mit besonderen Schwachstellen, wie den Registrierungstunnel zum RP, und stellen Sie sicher, dass der DR stets gut geschützt ist. CoPP ist in diesen Bereichen sehr hilfreich.

4. Wenn domänenübergreifende ASM-Services erforderlich sind, überlegen Sie, ob BiDir PIM bereitgestellt werden kann.
5. Verwenden Sie globale mroute/igmp-Statusgrenzen - verstehen Sie die Funktionen Ihrer Plattformen sowie die erwartete maximale Anzahl an Status, die Sie unter normalen Umständen und im schlimmsten Fall benötigen. Konfigurieren Sie Grenzen innerhalb der Funktionen Ihrer Plattform, die es Ihrem Netzwerk ermöglichen, seine maximalen Grenzen zu erreichen.
6. Grundlegende Filter: rACL/CoPP und Infrastruktur-ACLs blockieren PIM auf dem Access Layer

IP-Multicast ist ein leistungsstarkes und skalierbares Mittel zur Bereitstellung einer Vielzahl von Anwendungsservices. Wie bei Unicast muss auch hier eine Vielzahl unterschiedlicher Bereiche geschützt werden. In diesem Dokument werden die grundlegenden Bausteine zum Sichern eines IP-Multicast-Netzwerks beschrieben.

Zugehörige Informationen

- Richtlinien für die Zuweisung von IP-Multicast-Adressen
- Konfigurieren von IPv4-IGMP-Filtern
- Gruppenverschlüsseltes Transport-VPN

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.