Implementaciones de multidifusión IP seguras

Contenido

Introducción

Este documento describe las directrices generales sobre las prácticas recomendadas para proteger una infraestructura de red de multidifusión IP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IP Multicast

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento cubre algunos conceptos básicos, terminología, y discute los temas listados:

- Mecanismos para proteger una plataforma específica y la red en general.
- Cualquier modelo de multidifusión de origen (ASM) y multidifusión específica de origen (SSM).
- Seguridad de red privada virtual (MVPN) multidifusión.
- Arquitectura de red privada virtual (VPN) de transporte cifrado de grupo (GET) que

proporciona confidencialidad e integridad para el tráfico del plano de control o de datos de multidifusión.

Terminology

En la multidifusión IP hay dos modelos de servicio clásicos:

1. Cualquier multidifusión de origen (ASM)

2. Multidifusión por fuente específica (SSM)

En ASM, el receptor se une a un grupo G mediante un informe de pertenencia al protocolo de pertenencia a grupos de Internet (IGMP) o a Multicast Listener Discovery (MLD) para indicar el grupo. Este informe solicita el tráfico enviado por cualquier origen al grupo G y, por lo tanto, el nombre "cualquier origen". Por el contrario, en SSM, el receptor se une a un canal específico definido por una fuente S, que envía a un grupo G. Cada uno de estos modelos de servicio se describe en detalle a continuación.

Cualquier multidifusión de origen

El modelo de ASM se caracteriza por dos clases de protocolo: "dense mode flood-and-prune" y "sparse mode explicit join":

i) Protocolos de saturación y eliminación en modo denso (DVMRP/MOSPF/PIM-DM)

En los protocolos de modo denso, todos los routers de la red son conscientes de todos los árboles, sus orígenes y receptores. Protocolos como el protocolo de routing multidifusión por vectores a distancia (DVMRP) y el modo denso de multidifusión independiente del protocolo (PIM) saturan la información de "fuente activa" en toda la red y crean árboles mediante la creación del "estado de separación" en partes de la topología en las que el tráfico de un árbol específico no es deseado. También se les llama protocolos de inundación y ciruela. En Multicast Open Shortest Path First (MOSPF), la información sobre los receptores se inunda a través de la red para permitir la creación de árboles.

Los protocolos de modo denso no son deseables porque cada árbol construido en alguna parte de la red siempre puede causar la utilización de recursos (con impacto de convergencia) en todos los routers de la red (o dentro del alcance administrativo, si está configurado). Estos protocolos no se examinan más a fondo en el resto de este artículo.

ii) Protocolos de unión explícita en modo disperso (PIM-SM/PIM-BiDir)

Con los protocolos de unión explícita en modo disperso, los dispositivos no crean un estado específico de grupo en la red a menos que un receptor haya enviado un informe de afiliación (o "unión") IGMP/MLD explícito para un grupo. Se sabe que esta variante de ASM se amplía bien y es el paradigma de enfoque de multidifusión.

Esta es la base para el modo disperso de PIM, que la mayoría de las implementaciones multicast han utilizado hasta ahora. Esta es también la base de PIM bidireccional (PIM-BiDir), que se implementa cada vez más para MUCHAS (fuentes) en MUCHAS aplicaciones (receptores).

Estos protocolos se denominan modo disperso porque admiten eficazmente árboles de entrega

de multidifusión IP con una población de receptores "dispersos" y crean un estado de plano de control sólo en routers en la ruta entre orígenes y receptores, y en PIM-SM/BiDir, el punto de encuentro (RP). Nunca crean estado en otras partes de la red. El estado en un router sólo se genera explícitamente cuando recibe una unión de un router o receptor de flujo descendente, de ahí el nombre "protocolos de unión explícitos".

Tanto PIM-SM como PIM-BiDir utilizan "ÁRBOLES COMPARTIDOS", que permiten reenviar el tráfico de cualquier fuente a un receptor. El estado de multidifusión en un árbol compartido se denomina estado (*,G), donde * es un comodín para CUALQUIER ORIGEN. Además, PIM-SM admite la creación de estados relacionados con el tráfico de un origen específico. Estos se conocen como ÁRBOLES DE ORIGEN y el estado asociado se denomina estado (S,G).

Multidifusión desde un origen específico

SSM es el modelo utilizado cuando el receptor (o algún proxy) envía "uniones" (S,G) para indicar que desea recibir tráfico enviado por el origen S al grupo G. Esto es posible con los informes de pertenencia al modo "INCLUDE" de IGMPv3/MLDv2. Este modelo se denomina modelo de multidifusión desde un origen específico (SSM). SSM exige el uso de un protocolo de unión explícita entre routers. El protocolo estándar para esto es PIM-SSM, que es simplemente el subconjunto de PIM-SM utilizado para crear árboles (S,G). No hay ningún estado de árboles compartidos (*,G) en SSM.

De este modo, los receptores de multidifusión pueden "unirse" a un grupo G de ASM o "unirse" (o, más exactamente, "suscribirse") a un canal SSM (S,G). Para evitar la repetición del término "grupo ASM o canal SSM", se utiliza el término flujo (multidifusión), lo que implica que el flujo podría ser un grupo ASM o un canal SSM.

Protocolos de multidifusión/tipos de paquetes relevantes

Para proteger una red de multidifusión, es importante comprender los tipos de paquetes que se suelen encontrar y cómo protegerse frente a ellos. Hay tres protocolos principales que deben tenerse en cuenta:

1. IGMP/MLD
2. PIM
3. MSDP

En la siguiente sección, se discuten cada uno de estos protocolos y los problemas que pueden surgir con cada uno, respectivamente.

Paquetes IGMP/MLD

IGMP / MLD es el protocolo utilizado por los receptores de multidifusión para indicar a un router que desean recibir contenido para un grupo de multidifusión determinado. El protocolo de pertenencia a grupos de Internet (IGMP) es el protocolo que se utiliza en IPv4, y Multicast

Listener Discovery (MLD) es el protocolo que se utiliza en IPv6.

Hay dos versiones de IGMP que se implementan habitualmente, IGMPv2 e IGMPv3. También hay dos versiones de MLD que se implementan habitualmente, MLDv1 y MLDv2.

IGMPv2 y MLDv1 son funcionalmente equivalentes, e IGMPv3 y MLDv2 son funcionalmente equivalentes.

Estos protocolos se especifican en estos links:

IGMPv2: RFC 2236

MLDv1: RFC 3590

IGMPv3 y MLDv2: RFC 4604

IGMPv2 e IGMPv3 no es solo un protocolo, sino también un protocolo IPv4 IP (en concreto, el protocolo número 2). No sólo se utiliza como se describe en estos RFC para informar sobre la pertenencia a grupos de multidifusión, sino también por otros protocolos de multidifusión IPv4 como DVMRP, PIM versión 1, mtrace y mrinfo. Esto es importante recordarlo cuando intente filtrar IGMP (a través de ACL de Cisco IOS®, por ejemplo). En IPv6, MLD no es un protocolo IPv6; en su lugar, ICMPv6 se utiliza para transportar paquetes MLD. La versión 2 de PIM es el mismo tipo de protocolo en IPv4 e IPv6 (número de protocolo 103).

Paquetes de control PIM

En esta sección, se analizan los paquetes de control PIM de multidifusión y unidifusión. Se discuten tanto el RP automático como el Bootstrap Router (BSR), que son formas de seleccionar puntos de encuentro y controlar las asignaciones de grupo a RP en redes PIM-SM.

Paquetes de control PIM de multidifusión

Los paquetes de control PIM de multidifusión incluyen:

- **PIM Hello** - El paquete PIM Hello es un paquete de multidifusión IP de alcance local de link enviado a un router conectado a la misma red para establecer vecinos PIM.
- **PIM Join/Prune** - Las PIM Join/Prunes son paquetes de multidifusión IP de alcance local de link enviados para crear/quitar el estado de multidifusión y sólo se envían a los vecinos PIM. Son multidifusión dentro de la LAN para facilitar la aserción, la supresión de informes y otros detalles del protocolo PIM, pero siempre se dirigen a un vecino específico.
- **PIM DF-elect** - PIM Designated Forwarder es el router PIM Bi-Dir responsable de (*,G) JOINS enviados al RP en nombre de receptores conectados o vecinos PIM descendentes. Para los casos en que un router PIM detecta otro router que envía (*,G) JOINS en el mismo segmento para el mismo grupo G, hay una elección para determinar el router con la mejor trayectoria al RP.
- **PIM Assert** - Las PIM Assert son paquetes multicast IP locales de link enviados cuando un router PIM conectado a un segmento de red que reenvía activamente paquetes para un determinado (S,G) fuera de una interfaz particular comienza a RECIBIR paquetes para ese

mismo (S,G) en la misma interfaz en la que se reenvían. Este evento indica la presencia de otro router que piensa que es el reenviador único (SF) para este (S,G). El mecanismo Assert elige un SF único para eso (S,G). El router PIM SF se elige para reenviar paquetes para un flujo (S,G) determinado. PIM permite que diferentes routers realicen la función del SF en nombre de diferentes (S,G)s, idealmente solo hay un SF por (S,G). No confunda el SF con el router designado. El router designado PIM es el router responsable de JOIN / PRUNES o SOURCE REGISTERS que se envían al RP en una red PIM-SM.
- **PIM Bootstrap** - Los mensajes PIM Bootstrap se envían en una red PIMv2 para facilitar la elección dinámica de un punto de encuentro para un grupo G determinado.

Paquetes de control PIM unidifusión

Los paquetes de control PIM unidifusión se dirigen hacia o desde el RP e incluyen:

- **Source Register Packet** - Los paquetes de registro de origen PIM se envían para registrar un nuevo origen multicast con un punto de encuentro. Tan pronto como un Origen comienza a enviar paquetes multicast, el Router designado que está conectado a la red de origen envía un flujo de registro unicast al RP para indicar que hay un origen activo presente para un grupo multicast del cual el RP es responsable.
  Los paquetes de registro de origen se envían como una encapsulación unicast del flujo multicast original.
  Los mensajes de registro PIM son conmutados a nivel de proceso y se envían solamente hasta que el RP envía un mensaje de detención de registro. El impacto en el rendimiento de estos paquetes es proporcional a la velocidad de la fuente (por flujo (S,G)).
- **Register Stop Packet** - PIM Register Stop Los paquetes se envían desde el punto de encuentro al PIM DR que envió el mensaje de registro. Los mensajes de Detención de Registro se envían tan pronto como el RP comienza a recibir paquetes multicast de forma nativa desde el origen.
- **Paquetes de Anuncio de Punto de Encuentro de Candidatos BSR** - PIM BSR Los paquetes de Anuncio C-RP se envían al BSR para anunciar un RP candidato una vez que se elige el BSR.

Figura 1: Paquetes unidifusión PIM

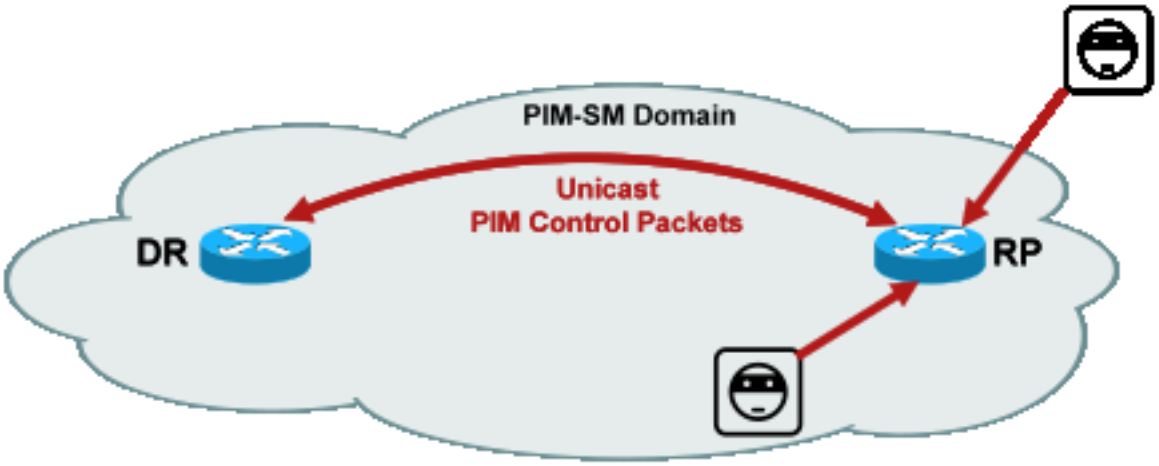

Fig1

_PIM_unicast

Los ataques que explotan estos paquetes pueden originarse en cualquier lugar, ya que estos paquetes son de unidifusión.

Paquetes RP automáticos

Auto-RP es un protocolo desarrollado por Cisco que tiene el mismo propósito que PIMv2 BSR. Auto-RP fue desarrollado antes de BSR, y sólo soporta IPv4. BSR soporta IPv4 e IPv6. El Mapping Agent en Auto-RP sirve la misma función que el router bootstrap en BSR. En BSR, los mensajes del C-RP son unicast al router bootstrap. En RP automático, los mensajes se envían a través de multidifusión al agente de asignación, lo que permite filtros más sencillos en el límite, como se describe más adelante. El RP automático se describe en detalle en este enlace: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

En Cisco IOS, los paquetes AutoRP/BSR siempre se reenvían y actualmente no están inhabilitados. Esto puede presentar una exposición de seguridad particular en el caso de RP automático.

Figura 2: Paquetes RP automáticos

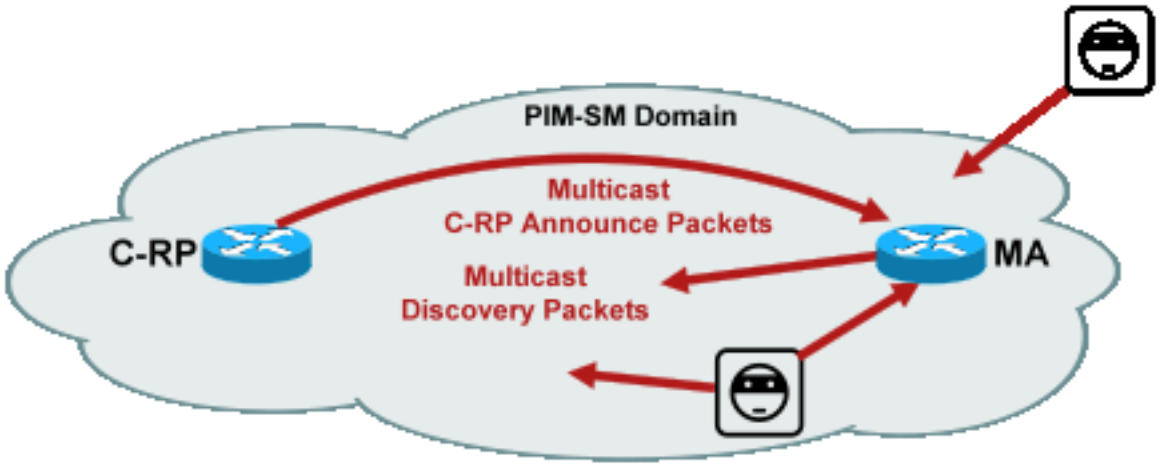

Fig2_A

utoRP_packets

Nota: Aunque Auto-RP se utiliza como mecanismo para el anuncio y la detección de PIM-SM RP, no utiliza paquetes PIM (protocolo IP 103); en su lugar, utiliza paquetes del puerto 496 del protocolo de datagramas de usuario (UDP) con direcciones de multidifusión.

Existen dos tipos de paquetes que utiliza Auto-RP:

- Paquetes C-RP-Announce: estos paquetes son multidifusión para todos los agentes de asignación y utilizan una dirección "conocida" reservada de la Autoridad de números asignados de Internet (IANA) (224.0.1.39). Son enviados por un C-RP para anunciar la dirección RP y el rango de grupo para los cuales ese RP puede actuar como RP.
- Paquetes de detección de C-RP: estos paquetes son multidifusión a todos los routers PIM y utilizan una dirección "conocida" reservada IANA (224.0.1.40). El agente de asignación de RP automático los envía para anunciar el RP-C específico que se selecciona como RP para un rango de grupo determinado.

Cada uno de estos tipos de paquetes está destinado a ser inundado a través de la red.

En Cisco IOS, tanto 224.0.1.39 como 224.0.1.40 se reenvían en modo denso PIM para evitar un problema de no conocimiento previo del RP para un grupo cuando ese grupo se utiliza para distribuir información RP. Este es el único uso recomendado del modo denso PIM.

En Cisco IOS XR, los mensajes de RP automático se inundan salto por salto de vecino a vecino con reenvío de ruta inversa (RPF). Por lo tanto, no es necesario crear un estado de ruta multicast PIM DM para soportar Auto-RP en Cisco IOS XR. De hecho, Cisco IOS XR no admite PIM-DM en absoluto.

Paquetes de protocolo de detección de servicios multidifusión (MSDP)

MSDP es el protocolo IPv4 que permite que una fuente en un dominio sea anunciada a un receptor en otro dominio a través de sus respectivos puntos de encuentro. MSDP se especifica en RFC 3618.

Para compartir información sobre orígenes activos entre dominios PIM, se utiliza MSDP. Si un origen se activa en un dominio, MSDP se asegura de que todos los dominios de peer aprendan sobre este nuevo origen de manera oportuna, lo que permite que los receptores en otros dominios hagan contacto rápidamente con este nuevo origen si resulta que se ha enviado a un grupo en el que los receptores tienen interés. MSDP es necesario para las comunicaciones de multidifusión de ASM/PIM-SM y se ejecuta a través de una conexión de protocolo de control de transporte (TCP) de unidifusión configurada entre puntos de encuentro en los dominios respectivos.

Amenazas en un entorno de multidifusión

Zonas de confianza y límites de confianza

Esta sección del documento está organizada por entidades funcionales de la red. El modelo de amenazas que se ha analizado se basa en estas entidades. Por ejemplo, este documento explica cómo se puede proteger un router en una red multicast (desde un punto de vista multicast), independientemente de dónde esté implementado el router. Del mismo modo, hay consideraciones sobre cómo implementar medidas de seguridad en toda la red, o medidas en un router designado, punto de encuentro, etc

Las amenazas descritas aquí también siguen esta lógica y están organizadas por función lógica en la red.

Descripción general de amenazas

En un nivel abstracto, cualquier implementación de multidifusión puede estar sujeta a una serie de amenazas en diversos aspectos de la seguridad. Los aspectos clave de la seguridad son la confidencialidad, la integridad y la disponibilidad.

- **Amenazas contra la confidencialidad**: En la mayoría de las aplicaciones, el tráfico de multidifusión no está cifrado y, por lo tanto, está abierto a cualquier persona que escuche o capture en cualquier línea o elemento de red de la ruta. En la sección sobre GET VPN, se discuten las formas de cifrar el tráfico multicast para evitar dichos ataques.
- **Amenazas contra la integridad del tráfico**: Sin seguridad a nivel de aplicación o seguridad basada en red, como VPN GET, el tráfico multidifusión es vulnerable a modificaciones en tránsito. Esto es particularmente importante para el tráfico del plano de control que utiliza multidifusión, como OSPF, PIM y muchos otros protocolos.
- **Amenazas contra la integridad de la red**: Sin los mecanismos de seguridad descritos en este documento, los remitentes, receptores o elementos de red comprometidos que no estén autorizados pueden acceder a la red de multidifusión, enviar y recibir tráfico sin autorización (robo del servicio) o sobrecargar los recursos de red.
- **Amenazas contra la disponibilidad**: Existen diversas posibilidades de ataques de denegación de servicio que pueden hacer que los recursos no estén disponibles para los usuarios legítimos.

En las siguientes secciones se tratan las amenazas para cada función lógica de la red.

Amenazas básicas contra un router

Existen varias amenazas fundamentales contra un router que son independientes de si el router admite la multidifusión y de si el ataque implica tráfico o protocolos de multidifusión.

Los ataques de denegación de servicio (DoS) son los vectores de ataque genéricos más importantes de una red. En principio, todos los elementos de la red pueden ser objetivo de un ataque de DoS, que puede sobrecargar el elemento con una posible pérdida o degradación del servicio para los usuarios legítimos. Es de vital importancia seguir las recomendaciones básicas de seguridad de la red que se aplican a unicast.

Cabe destacar que los ataques de multidifusión no siempre son intencionales, sino que a menudo son accidentales. Por ejemplo, el gusano Witty, observado por primera vez en marzo de 2004, es un ejemplo de un gusano que se propaga a través de ataques aleatorios en direcciones IP. Como consecuencia de la aleatorización completa del espacio de direcciones, los destinos IP de multidifusión también se vieron afectados por el gusano. En muchas organizaciones, varios routers de primer salto colapsaron porque el gusano envió paquetes a muchas direcciones de destino multidifusión diferentes. Los routers, sin embargo, no fueron diseñados para tal carga de tráfico multicast con la creación de estado asociada, y experimentaron efectivamente agotamiento de recursos. Esto ilustra la necesidad de proteger el tráfico de multidifusión, incluso si esta no se utiliza en una empresa.

Las amenazas genéricas contra los routers incluyen:

- Inundaciones de paquetes de cualquier tipo; por ejemplo, en rutas de hardware como rutas lentas (punt) y rutas de software como puertos del plano de control o de administración, que incluyen Secure Shell (SSH), Telnet, protocolo de gateway fronterizo (BGP), OSPF, protocolo de tiempo de red (NTP), etc
- Intrusiones en el router, con explotación posterior de las funciones del router; las contraseñas Telnet o SSH débiles y las cadenas de comunidad SNMP (Simple Network Management Protocol) débiles son un problema común en las redes modernas.
- Los problemas operativos, como los errores de configuración o los ataques internos, pueden poner en peligro la seguridad de toda la red y su tráfico.

Cuando la multidifusión está activada en un router, debe protegerse además de la unidifusión. El uso de la multidifusión IP no cambia el modelo de amenaza fundamental; sin embargo, habilita protocolos adicionales (PIM, IGMP, MLD, MSDP) que podrían estar sujetos a ataques, que deben protegerse específicamente. Cuando se utiliza tráfico de unidifusión en estos protocolos, el modelo de amenaza es idéntico a otros protocolos que ejecuta el router.

Es importante tener en cuenta que el tráfico de multidifusión no se puede utilizar del mismo modo que el tráfico de unidifusión para atacar un router porque el tráfico de multidifusión está fundamentalmente "dirigido por el receptor" y no se puede dirigir a un destino remoto. Un objetivo de ataque debe "unirse" explícitamente a la secuencia de multidifusión. En la mayoría de los casos (el RP automático es la excepción principal), los routers solo escuchan y reciben tráfico

multicast "local de link". El tráfico local de enlace nunca se reenvía. Por lo tanto, los ataques en un router con paquetes de multidifusión sólo pueden originarse en atacantes conectados directamente.

Amenazas desde el lado del origen

Las fuentes de multidifusión, ya sean PC o servidores de vídeo, a veces no están bajo el mismo control administrativo que la red. Por lo tanto, desde el punto de vista del operador de red, el remitente se trata principalmente como no fiable. Dadas las potentes capacidades de los PC y los servidores, y su compleja configuración de seguridad, que a menudo es incompleta, los remitentes suponen una importante amenaza para cualquier red, incluida la multidifusión. Estas amenazas incluyen:

- **Ataques de capa 2:** existe una amplia gama de formas de ataque en la capa 2 para llevar a cabo diversos tipos de ataques. Se aplican tanto a unidifusión como a multidifusión. Dado que estos formularios de ataque no son específicos de la multidifusión, no se tratan con más detalle en este documento. Para obtener más información, consulte el libro de Cisco Press "LAN Switch Security", ISBN-10: 1-58705-467-1.
- **Ataques con tráfico multicast:** Como se describió anteriormente, es difícil realizar ataques con tráfico multicast ya que el router de primer salto no reenvía tráfico multicast a menos que haya un receptor para el grupo. Sin embargo, el primer salto puede ser atacado de varias maneras con los paquetes multicast:
- Ataques de saturación de red: Un atacante puede inundar un segmento con paquetes de multidifusión, sobre la utilización del ancho de banda disponible, lo que puede llevar a una condición de DoS.
- Ataques de estado de multidifusión: El router de primer salto está inundado de paquetes de multidifusión, que pueden crear demasiado estado y una condición de ataque de DoS consiguiente.
- Un remitente podría intentar convertirse en PIM DR a través de los saludos PIM que se envían. En estos casos, ningún tráfico se reenviaría hacia o desde la LAN.
- Los paquetes de elección PIM DF para un BiDir-PIM DF podrían ser falsificados. En estos casos, ningún tráfico se reenviaría hacia o desde la LAN.
- Un remitente podría falsificar mensajes de detección RP automática o de arranque BSR. Esto anunciaría efectivamente un RP falso, y haría caer o interrumpiría un servicio PIM-SM/BiDir.
- Un remitente podría originar ataques de unidifusión, como mensajes de registro/registro-detención de origen PIM, o podría enviar paquetes de anuncio BSR y anunciar un BSR falso.
- Un remitente puede enviar a cualquier grupo de multidifusión válido, a menos que se filtre. Si una dirección de origen se falsifica y no se impide en el extremo, el remitente puede utilizar la dirección IP de origen de un remitente legítimo y reemplazar el contenido en partes de la red.
- Ataques de multidifusión contra protocolos del plano de control: Varios protocolos no asociados con la multidifusión, como OSPF y el protocolo de configuración dinámica de host (DHCP), utilizan paquetes de multidifusión, que se pueden utilizar para atacar estos protocolos
- **Enmascaramiento:** hay una serie de formas de ataque en las que un remitente puede fingir ser otro remitente. Las direcciones IP de origen falsificadas son una de esas formas de ataque.
- **Robo de servicio:** a menos que los remitentes estén controlados, es posible utilizar el servicio

de multidifusión de forma ilegítima desde el lado del remitente.

Nota: Los hosts normalmente no envían ni reciben paquetes PIM. El host que lo hace probablemente puede intentar un ataque.

Amenazas desde el lado del receptor

El receptor también suele ser una plataforma con una potencia de CPU y un ancho de banda significativos, y admite diversas formas de ataque. En su mayoría, son idénticas a las amenazas del lado del remitente. Los ataques de capa 2 siguen siendo un importante vector de ataque. Los receptores falsos y el robo del servicio también son posibles en el lado del receptor, excepto que el vector de ataque es normalmente IGMP (o ataques de capa 2, como se mencionó).

Amenazas contra un punto de encuentro y BSR

Los RP PIM-SM y PIM-BSR son puntos críticos en una red multicast y, por lo tanto, son objetivos valiosos para un atacante. Cuando ninguno de los dos es el router de primer salto, sólo los formularios de ataque de unidifusión, que incluyen unidifusión PIM, pueden ser dirigidos directamente contra esos elementos. Las amenazas contra RP y BSR incluyen:

- Todos los formularios de ataque genéricos, como se describe en la sección "Amenazas básicas contra un router".
- Los ataques de unidifusión PIM, potencialmente con direcciones IP de origen falsificadas, permiten ataques de DoS, a través de mensajes de registro PIM o de detención de registro enviados por un dispositivo malicioso.

Seguridad multidifusión y unidifusión (comparada)

Consideraciones/filtros de estado

Considere la topología de la figura 3, que muestra una fuente, tres receptores (A, B, C), un switch (S1) y dos routers (R1 y R2). La línea azul representa una secuencia de unidifusión y la línea roja representa una secuencia de multidifusión. Los tres receptores son miembros del flujo de multidifusión.

Figura 3: Replicación en routers y switches

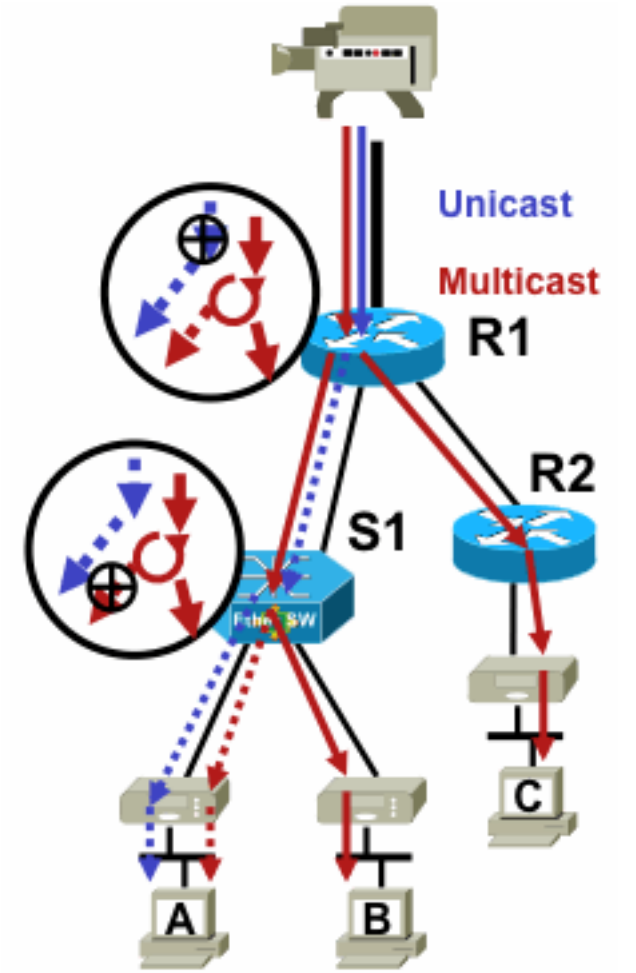

Fig3_replication_RS

Para inhibir el flujo de tráfico de un origen específico a un receptor específico:

- Para la secuencia de unidifusión, instale un filtro en cualquier lugar de la ruta de acceso del remitente al destinatario.
- Sin embargo, para la secuencia de multidifusión, los administradores deben ser más específicos acerca de dónde instalar los filtros: en el filtro del lado del receptor después del último punto de replicación antes del receptor; en el filtro de origen antes del primer punto de replicación después del origen.

Ataques desde fuentes de multidifusión

Esta sección se aplica a los modelos de servicio ASM y SSM, donde el tráfico se reenvía en función de la recepción de uniones explícitas del lado del receptor.

Para las secuencias de unidifusión no hay protección implícita del receptor. Un origen de unidifusión puede enviar tráfico a un destino, incluso si este destino no ha solicitado el tráfico. Por lo tanto, los mecanismos de defensa, como los firewalls, se suelen utilizar para proteger los terminales. Por otra parte, la multidifusión tiene una protección implícita integrada en los protocolos. Idealmente, el tráfico solo llega a un receptor que se ha unido al flujo en cuestión.

Con ASM, los orígenes pueden iniciar la inserción de tráfico o ataques de DoS a través de la transmisión de tráfico multidifusión a cualquiera de los grupos admitidos por un RP activo. Idealmente, este tráfico no llega a un receptor, pero puede alcanzar el router de primer salto en la trayectoria como mínimo, así como el RP, que permite ataques limitados. Sin embargo, si una fuente maliciosa conoce un grupo al que está interesado un receptor objetivo y no existen filtros adecuados, puede enviar tráfico a ese grupo. Este tráfico se recibe siempre y cuando los receptores escuchen al grupo.

Con SSM, los ataques por fuentes no deseadas sólo son posibles en el router de primer salto donde el tráfico se detiene si ningún receptor se ha unido a ese canal (S,G). Esto no conduce a ningún ataque de estado en el router de primer salto porque descarta todo el tráfico SSM para el cual no existe ningún estado de unión explícito de los receptores. En este modelo, no es suficiente que una fuente malintencionada sepa a qué grupo está interesado un objetivo porque las "uniones" son específicas del origen. Aquí, las direcciones IP de origen que son simuladas más los posibles ataques de ruteo serían necesarios para tener éxito.

Ataques estatales

Incluso sin receptores presentes en una red, PIM-SM crea el estado (S,G) y (*,G) en el router de primer salto más cercano al origen y también en el punto de encuentro. Por lo tanto, existe la posibilidad de un ataque de estado en la red en el router de primer salto de origen y en el RP PIM-SM.

Si un origen malicioso comienza a enviar tráfico a varios grupos, para cada uno de los grupos que se detectan, los routers en el estado de creación de red en el origen y el RP, siempre que los grupos en cuestión estén permitidos por la configuración RP.

Por lo tanto, PIM-SM está sujeto a ataques de estado y tráfico por parte de las fuentes. El ataque se puede agravar si el origen cambia su dirección IP de origen aleatoriamente dentro del prefijo correcto, o en otras palabras, sólo se simulan los bits de host de la dirección.

Figura 4: Ataques RP de ASM

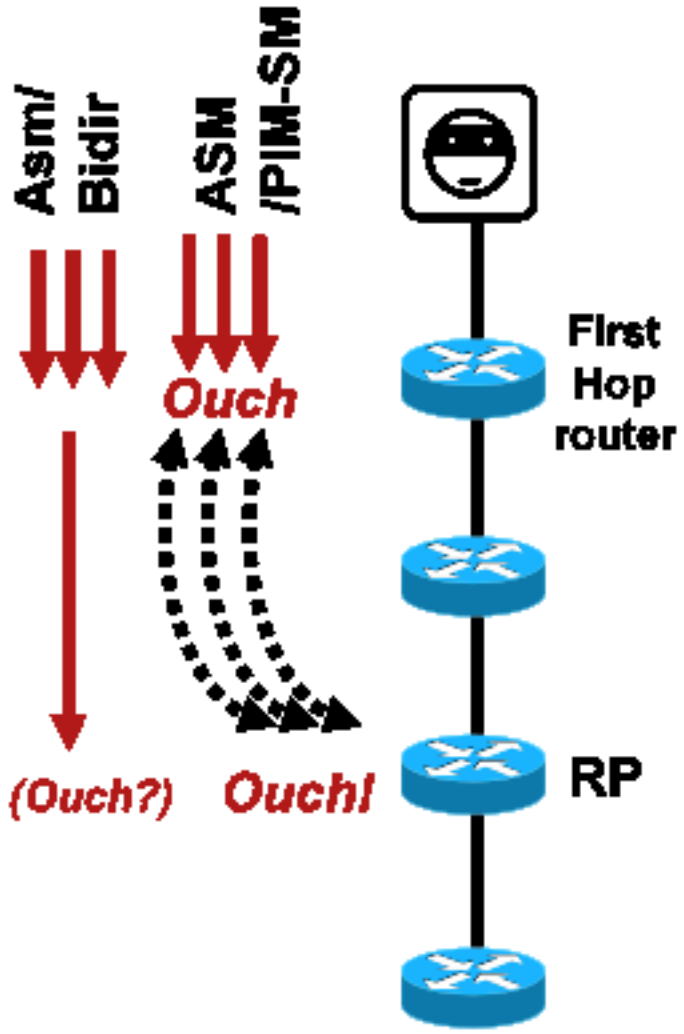

Fig4_ASM_RP_Attacks

Al igual que con PIM-SSM, los ataques de creación de estado PIM-BiDir desde fuentes son imposibles. El tráfico en PIM-BiDir se reenvía en el estado creado por las uniones de los receptores así como en el tráfico reenviado del estado al RP, de modo que pueda alcanzar a los receptores detrás del RP, ya que las uniones solamente van al RP. El tráfico de estado a reenvío al RP se denomina estado (*,G/M) y se crea mediante la configuración RP (estática, RP automático, BSR). No cambia en presencia de fuentes. Por lo tanto, los atacantes pueden enviar tráfico multidifusión a un RP PIM-BiDir, pero a diferencia de PIM-SM, un RP PIM-BiDir no es una entidad "activa" y, en su lugar, solo reenvía o descarta tráfico para los grupos PIM-BiDir.

> **Nota:** En algunas plataformas Cisco IOS (*,G/M), el estado no es compatible. En estos casos, los orígenes pueden atacar al router mediante la transmisión de tráfico multidifusión a varios grupos PIM-BiDir, lo que provoca la creación de estado (*,G). Por ejemplo, el switch Catalyst 6500 admite estados (*,G/M).

Ataques iniciados por el receptor

Los ataques pueden originarse en receptores de multidifusión. Cualquier receptor que envíe informes IGMP/MLD normalmente crea el estado en el router de primer salto. No existe un mecanismo equivalente en unidifusión.

Figura 5: Reenvío explícito de tráfico basado en la conexión del lado receptor

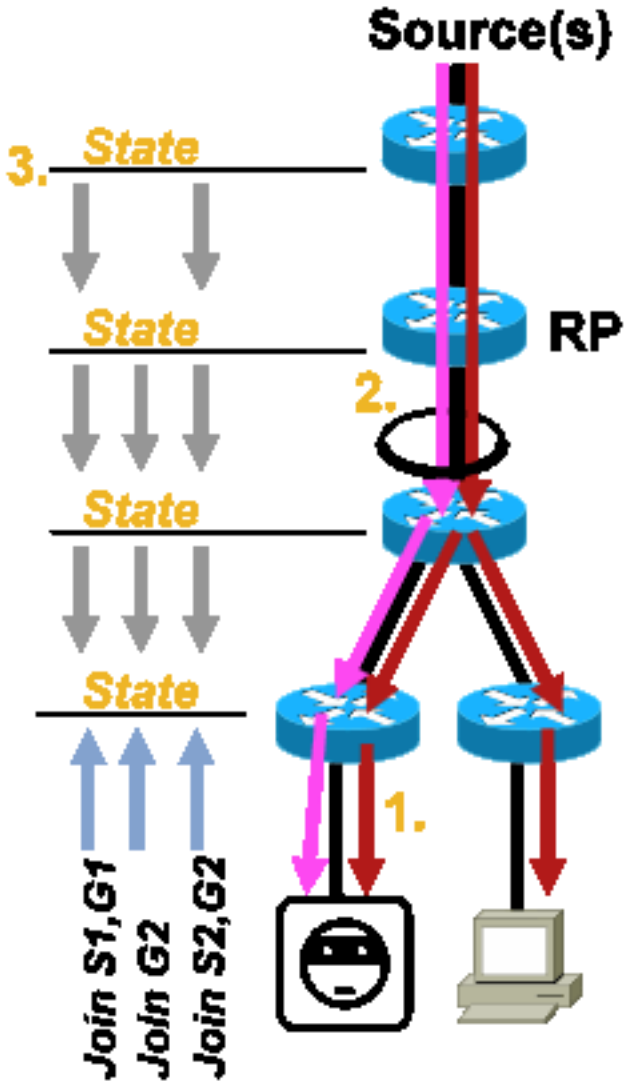

Fig5_Receiver_Explicit_Join

Los ataques de receptor pueden ser de tres tipos:

1. Un receptor de multidifusión puede intentar unirse a un flujo para el que no está autorizado e intentar recibir contenido que no está autorizado a recibir.
2. Un receptor de multidifusión puede sobrecargar potencialmente el ancho de banda de red disponible a través del interés en muchos grupos o canales. Este tipo de ataque se convierte en un ataque de ancho de banda compartido contra otros receptores potenciales de contenido.
3. Un receptor de multidifusión puede intentar iniciar un ataque contra routers o switches. Se puede generar un gran número de informes IGMP, lo que puede crear una gran cantidad de estado de árbol de multidifusión y sobrecargar potencialmente la capacidad del router. Esto, a su vez, puede resultar en un aumento de los tiempos de convergencia de multidifusión o en un DoS en el router.

En la siguiente sección, Seguridad dentro de una red de multidifusión, encontrará diversas formas de mitigar este tipo de ataques.

Seguridad en una red multidifusión

Seguridad de elementos de red

La seguridad no es una función puntual, sino una parte intrínseca de cada diseño de red. Como tal, la seguridad se debe tener en cuenta en cada punto de la red. Es de vital importancia que todos y cada uno de los elementos de la red estén protegidos de forma adecuada. Un posible escenario de ataque, aplicable a cualquier tecnología, es un router subvertido por un intruso. Una vez que un intruso tiene el control de un router, el atacante puede ejecutar una serie de escenarios de ataque diferentes. Por lo tanto, cada elemento de la red debe protegerse adecuadamente contra cualquier forma de ataque básico, así como contra ataques de multidifusión específicos.

Control Plane Policing (CoPP)

CoPP es la evolución de las ACL de router (rACL) y está disponible en la mayoría de las plataformas. El principio es el mismo: solo el tráfico destinado al router es controlado por CoPP.

La directiva de servicio utiliza la misma sintaxis que cualquier directiva de calidad de servicio, con mapas de directiva y mapas de clase. Por lo tanto, amplía la funcionalidad de rACL (permiso/denegación) con limitadores de velocidad para cierto tráfico hacia el plano de control.

> **Nota:** Ciertas plataformas, como los switches Catalyst de la serie 9000, tienen habilitado CoPP de forma predeterminada y la protección no se reemplaza. Consulte la guía de CoPP para obtener información adicional.

Si decide ajustar, modificar o crear rACL o CoPP en una red activa, debe tener cuidado. Dado que ambas funciones tienen la capacidad de filtrar todo el tráfico al plano de control, se deben permitir explícitamente todos los protocolos de plano de control y administración requeridos. La lista de protocolos requeridos es grande y puede ser fácil pasar por alto protocolos menos obvios como Terminal Access Controller Access Control System (TACACS). Todas las configuraciones de rACL y CoPP no predeterminadas deben probarse siempre en un entorno de laboratorio antes de la implementación en redes de producción. Además, las implementaciones iniciales deben comenzar únicamente con una política de "permisos". Esto permite la validación de cualquier resultado inesperado con los contadores de resultados de ACL.

En un entorno de multidifusión, los protocolos de multidifusión necesarios (PIM, MSDP, IGMP, etc.) deben estar permitidos en rACL o CoPP para que la multidifusión funcione correctamente. Es importante recordar que el primer paquete de una secuencia de multidifusión desde el origen en un escenario PIM-SM se utiliza como un paquete de plano de control para ayudar a crear el estado de multidifusión, en el plano de control del dispositivo. Por lo tanto, es importante permitir los grupos multicast relevantes en rACL o CoPP. Dado que existen varias excepciones específicas de la plataforma, es importante consultar la documentación pertinente y probar cualquier configuración planificada antes de la implementación.

Servicio de transporte de paquetes locales (LPTS)

En Cisco IOS XR, el Servicio de transporte de paquetes locales (LPTS) sirve como regulador del tráfico al plano de control del router, similar a CoPP en Cisco IOS. Además, el tráfico de recepción, que incluye el tráfico de unidifusión y multidifusión, se puede filtrar y limitar la velocidad.

Seguridad específica de multidifusión

En una red habilitada para multidifusión, cada elemento de red debe protegerse con características de seguridad específicas de multidifusión. Estos aspectos se describen en esta sección para la protección genérica del router. Las funciones que no son necesarias en todos los routers, pero solo en ubicaciones específicas de la red, y las funciones que requieren interacción entre routers (como la autenticación PIM) se analizan en la siguiente sección.

Límites de ruta multicast

El comando mroute limit limita la cantidad de rutas de multidifusión globalmente en un router y ayuda a evitar ataques de DoS.

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

Figura 6: Límites de ruta multicast

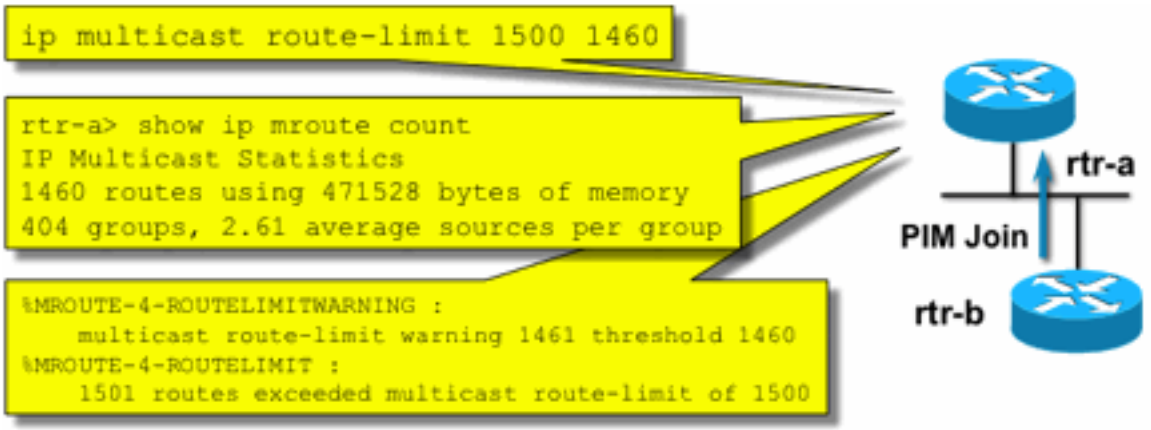

Fig6_Mroute_Limits

Los límites de ruta multicast permiten establecer un umbral en el número de rutas multicast que se permiten en la tabla de ruteo multicast. Si se habilita un límite de ruta multicast, no se crea ningún estado multicast más allá del límite configurado. También hay un umbral de advertencia. Cuando el número de rutas multicast excede el umbral de advertencia, se activan los mensajes de advertencia de syslog. En el límite de ruta multicast, cualquier paquete adicional que pueda activar el estado se descarta.

El comando **ip multicast route-limit** también está disponible por MVRF.

Desactivar escucha SAP: no ip sap listen

El comando **sap listen** hace que un router reciba mensajes de Protocolo de anuncio de sesión/Protocolo de descripción de sesión (SAP/SDP). SAP/SDP es un protocolo heredado que data de los días de la estructura básica de multidifusión (MBONE). Estos mensajes indican

información de directorio sobre el contenido de multidifusión que está disponible en el futuro o en la actualidad. Esto puede ser una fuente de un DoS contra la CPU del router y los recursos de memoria, y por lo tanto esta función debe ser inhabilitada.

Control del acceso a la información mrinfo: el comando "ip multicast mrinfo-filter"

El comando mrinfo (disponible en Cisco IOS y también en algunas versiones de Microsoft Windows y Linux) utiliza varios mensajes para consultar información a un router multicast. El comando de configuración global **ip multicast mrinfo-filter** se puede utilizar para limitar el acceso a esta información a un subconjunto de orígenes, o desactivarlo por completo.

Este ejemplo deniega las consultas originadas en 192.168.1.1, mientras que las consultas se permiten desde cualquier otro origen:

```
ip multicast mrinfo-filter 51

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

Este ejemplo niega *mrinfo* solicitudes de cualquier fuente:

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

> **Nota:** Como se esperaba con cualquier ACL, una *negación* significa que el paquete se filtra, mientras que un *permiso* significa que el paquete está permitido.

Si el comando **mrinfo** se utiliza para fines de diagnóstico, se recomienda configurar el comando **ip multicast mrinfo-filter** con una ACL apropiada para permitir consultas solamente de un subconjunto de direcciones de origen. La información proporcionada por el comando *mrinfo* también se puede recuperar a través de SNMP. Se recomienda encarecidamente realizar bloques completos de solicitudes mrinfo (bloquear cualquier origen de las consultas del dispositivo).

Seguridad de redes:

En esta sección se discuten varias maneras de asegurar los paquetes de control de multidifusión PIM y unidifusión, así como también Auto-RP y BSR.

Desactivar grupos de multidifusión

Los comandos **ip multicast group-range/ipv6 multicast group range** se pueden utilizar para inhabilitar todas las operaciones para los grupos denegados por la ACL:

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

Si aparecen paquetes para cualquiera de los grupos denegados por la ACL, se descartan en todos los protocolos de control, que incluyen PIM, IGMP, MLD, MSDP, y también se descartan en el plano de datos. Por lo tanto, nunca se crean entradas de caché IGMP/MLD, PIM, estado de

Base de información de ruteo de multidifusión/Base de información de reenvío de multidifusión (MRIB/MFIB) para estos rangos de grupo y todos los paquetes de datos se descartan inmediatamente.

Estos comandos se ingresan en la configuración global del dispositivo.

Se recomienda implementar este comando en todos los routers de la red, cuando y donde esté disponible, de modo que se controle todo el tráfico multicast que se origina fuera de la red. Tenga en cuenta que estos comandos afectan al plano de datos y al plano de control. Cuando está disponible, este comando proporciona una cobertura más amplia que las ACL estándar, y se prefiere.

Seguridad PIM

Control de vecino PIM

Un router PIM debe recibir saludos PIM para establecer la vecindad PIM. La vecindad PIM también es la base para la elección del router designado (DR) y la conmutación por error DR, así como para los mensajes PIM Join/Prune/Assert enviados/recibidos.

Figura 7: Control de vecino PIM

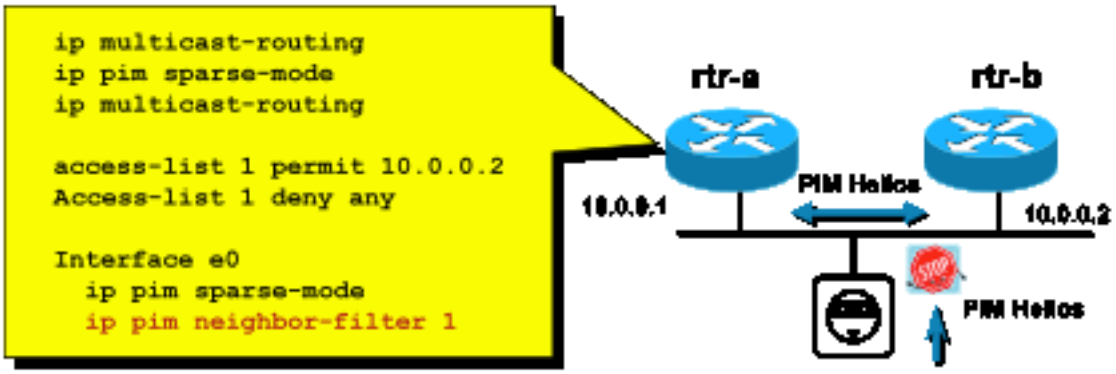

Fig7_PIM_neighbor_control

Para inhibir vecinos no deseados, utilice el comando **ip pim neighbor-filter** Este comando filtra todos los paquetes PIM de vecinos no permitidos, que incluyen Hellos, paquetes Join/Prune y paquetes BSR. Los hosts en el segmento pueden potencialmente falsificar la dirección IP de origen para fingir ser el vecino PIM. Se requieren mecanismos de seguridad de capa 2 (concretamente, protector de origen de IP) para evitar que las direcciones de origen sean objeto de un intento de simulación en un segmento o para utilizar una VLAN ACL en el switch de acceso con el fin de evitar paquetes PIM de hosts. La palabra clave "log-input" se puede utilizar en ACL para registrar paquetes que coinciden con la ACE.

El paquete PIM Join/Prune se envía a un vecino PIM para agregar o quitar ese vecino de una ruta de acceso determinada (S,G) o (*,G). Los paquetes de multidifusión PIM son paquetes de multidifusión local de vínculo enviados con un tiempo de vida (TTL)=1. Todos estos paquetes son de multidifusión a la dirección conocida de todos los routers PIM: 224.0.0.13. Esto significa que todos estos ataques deben originarse en la misma subred que el router atacado. Los ataques

pueden incluir paquetes Hello, Join/Prune y Assert falsificados.

> **Nota:** Un aumento o ajuste artificial del valor TTL en los paquetes multicast PIM a un valor mayor que 1 no crea problemas. La dirección de todos los routers PIM siempre se recibe y trata localmente en un router. Nunca es reenviado directamente por routers normales y legítimos.

Para proteger el RP contra una posible inundación de mensajes de registro PIM-SM, el DR necesita limitar la velocidad de esos mensajes. Utilice el comando **ip pim register-rate-limit**:

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

Figura 8: Control de túnel de registro PIM-SM

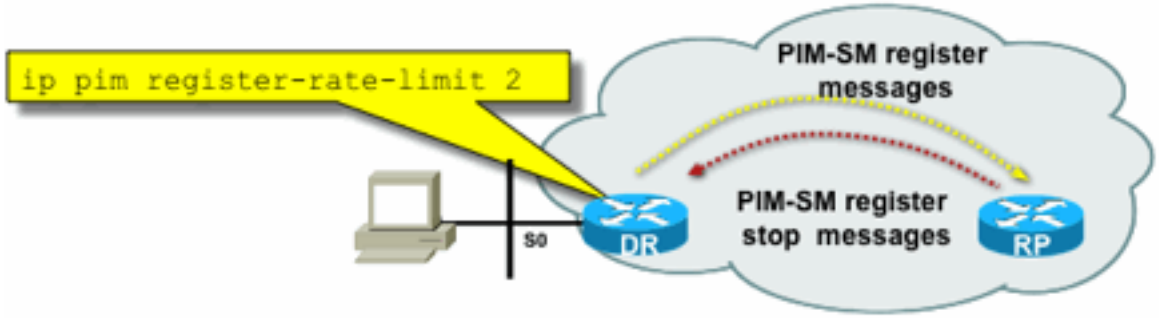

Fig8_PIMSM_Reg Tunnel

Los paquetes de unidifusión PIM se pueden utilizar para atacar el RP. Por lo tanto, el RP se puede proteger mediante ACL de infraestructura contra dichos ataques. Recuerde que los remitentes y receptores de multidifusión nunca necesitan enviar paquetes PIM, por lo que el protocolo PIM (protocolo IP 103) normalmente se puede filtrar en el extremo del suscriptor.

Control RP automático - Filtro de anuncio RP

El comando **ip pim rp-announce filter** es una medida de seguridad adicional que se puede configurar con RP automático siempre que sea posible:

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

Esto se puede configurar en el agente de mapeo para controlar qué routers se aceptan como RP candidatos para qué rangos de grupos / modo de grupo.

Figura 9: RP automático - Filtro de anuncio RP

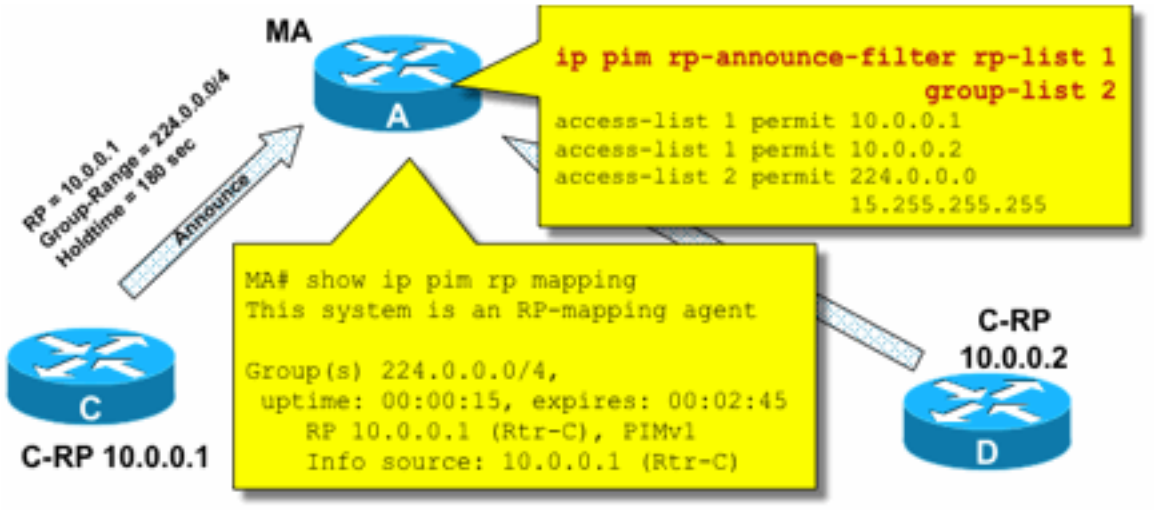

Fig9_AutoRP_RP_Announce

Control de RP Automático - Limitar Mensajes de RP Automático

Utilice el comando multicast border para restringir los paquetes AutoRP, RP-announce (224.0.1.39) o RP-discover (224.0.1.40) a un dominio PIM determinado:

```
ip multicast boundary
```

Figura 10: Comando de límite de multidifusión

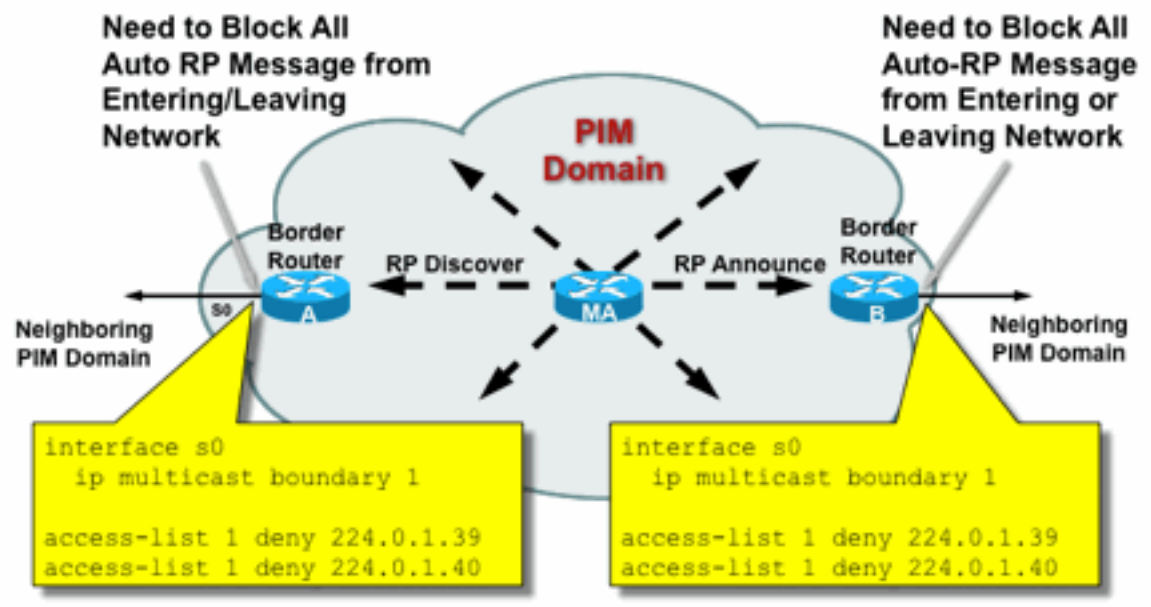

Fig10_Mcast_Boundary

Control BSR: limitar mensajes BSR

Use el comando **ip pim bsr-border** para filtrar mensajes BSR en el borde de un dominio PIM. No es necesaria ninguna ACL, ya que los mensajes BSR se reenvían salto a salto con la multidifusión local de link.

Figura 11: Borde BSR

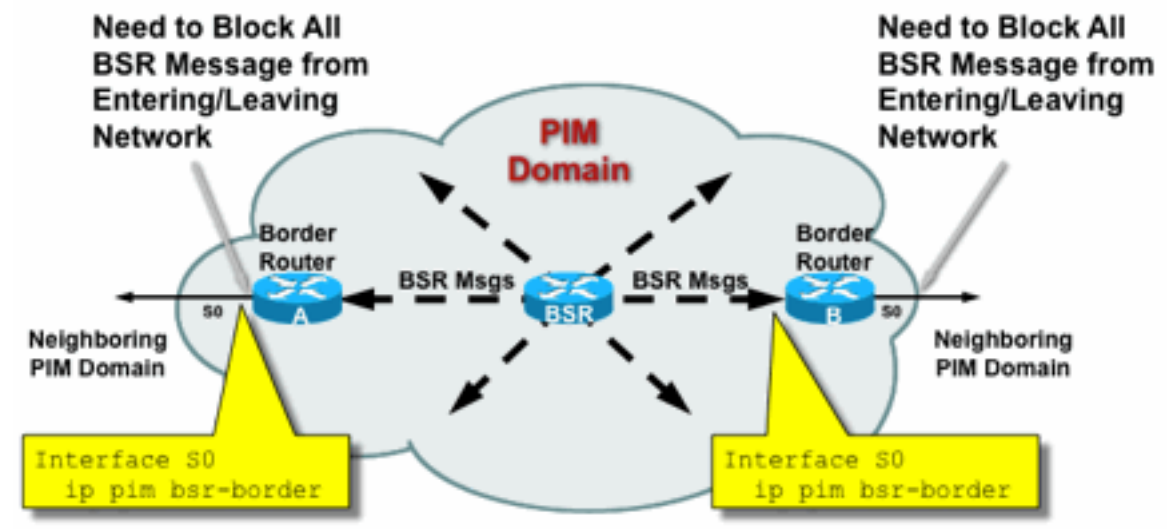

Fig11_BSR_Router

Filtros relacionados con RP/PIM-SM

Como parte de esta sección final, se discuten los filtros contra los paquetes de plano de control PIM-SP y RP, así como los mensajes Auto-RP, BSR y MSDP.

Filtros de RP automático

La figura 12 muestra un ejemplo de filtros de RP automático junto con ámbitos de dirección. Se muestran dos formas diferentes de enlazar una región. Las dos ACL son equivalentes desde una perspectiva de RP automático.

Figura 12: Filtros/alcances de RP automático

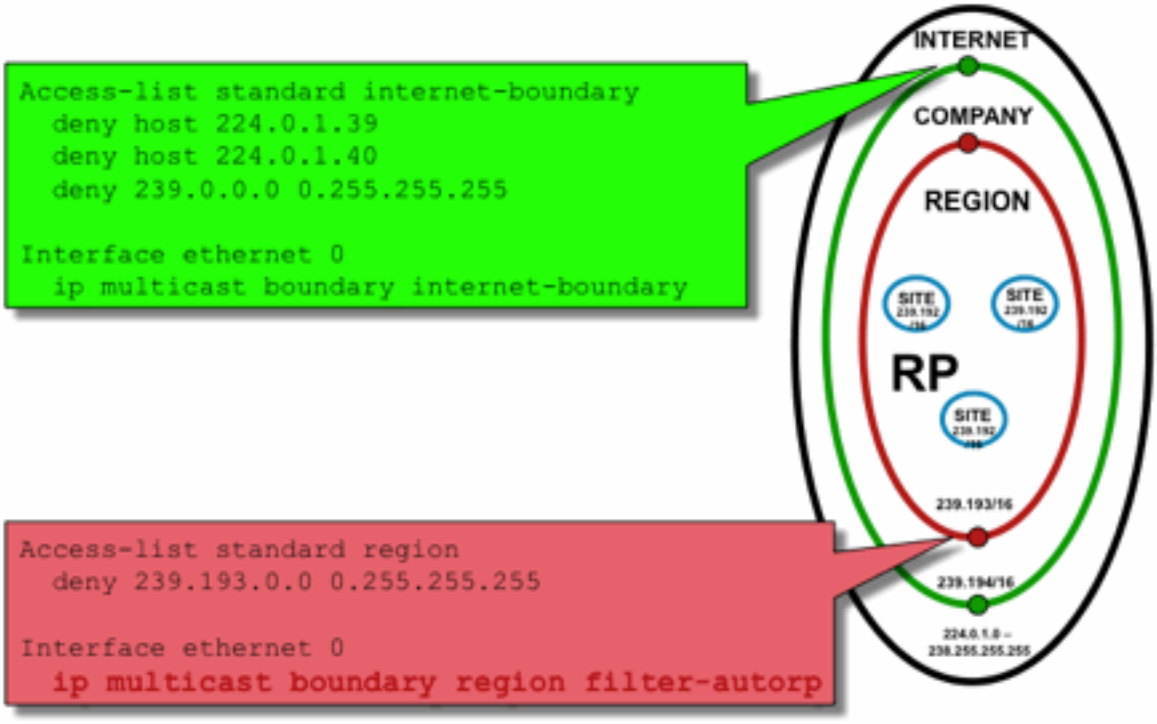

Fig12_AutoRP_Filtering_Scoping

La idea de los filtros de límite de la interfaz para RP automático es garantizar que los anuncios de RP automático solo lleguen a las regiones que admiten. Se definen los ámbitos regionales, empresariales e Internet, y en cada caso hay RP y anuncios de RP automático en cada ámbito. Los administradores solo quieren que los RP regionales sean conocidos por los routers regionales, que los RP de la empresa sean conocidos por los routers regionales y de la empresa, y que cualquier RP de Internet esté disponible globalmente. Es posible obtener más niveles de alcance.

Como se muestra en la imagen, hay dos maneras fundamentalmente diferentes de filtrar paquetes Auto-RP: El límite de Internet llama explícitamente a los grupos de control auto-rp (224.0.1.39 y 224.0.1.40), lo que resulta en filtros contra todos los paquetes Auto-RP. Este método se puede utilizar en el borde de un dominio administrativo, donde no se transfieren paquetes de RP automático. El límite de región utiliza la palabra clave filter-auto-rp para hacer un examen de los anuncios rp-to-group-range dentro de los paquetes RP automáticos. Cuando la ACL niega explícitamente un anuncio, se lo quita del paquete RP automático antes de que se reenvíe el paquete. En el ejemplo, esto permite que los RP de toda la empresa se conozcan dentro de las regiones, mientras que los RP de toda la región se filtran en el límite desde la región hasta el resto de la empresa.

Filtros entre dominios y MSDP

En este ejemplo, ISP1 actúa como proveedor de tránsito PIM-SM. Solo admiten el peering MSDP con vecinos y solo aceptan (S,G), pero no (*,G) tráfico en los routers de borde.

En interdominios (generalmente entre sistemas autónomos) hay dos medidas básicas de seguridad a tomar:

1. Proteja el plano de datos mediante el comando **multicast border**. Esto garantiza que el tráfico de multidifusión sólo se acepte para grupos definidos (y posibles orígenes).
2. Proteja el tráfico del plano de control entre dominios (MSDP). Se trata de una serie de medidas de seguridad independientes: Control de contenido MSDP, limitación de estado y autenticación de vecinos.

La Figura 13 proporciona un ejemplo de configuración de un filtro de interfaz en uno de los routers de borde de ISP1.

Para asegurar el plano de datos en el límite de dominio que inhibe las uniones (*,G) mediante filtros contra "host 0.0.0.0" y direcciones con ámbito administrativo mediante el comando **multicast border**:

Figura 13: Filtro entre dominios (*,G)

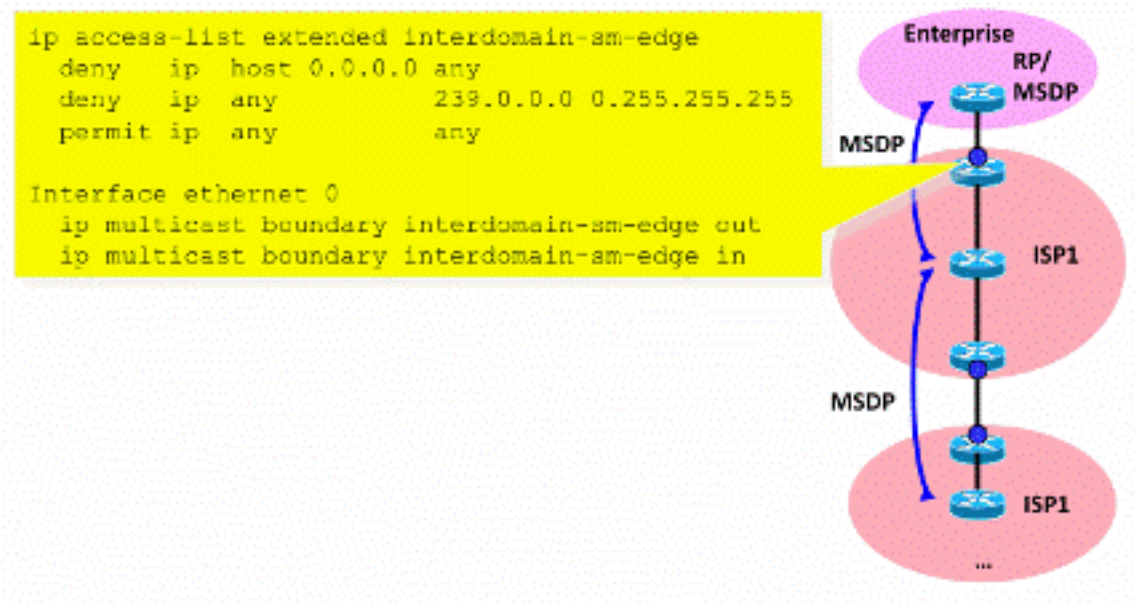

Fig13_Interdomain_Filter

Para asegurar el plano de control, fortalezca MSDP a través de tres medidas de seguridad básicas:

1) Filtros SA MSDP

Es una "práctica común recomendada" filtrar el contenido de los mensajes MSDP mediante filtros MSDP SA. La idea principal de este filtro es evitar la propagación del estado de multidifusión para aplicaciones y grupos que no son aplicaciones de Internet y no necesitan reenviarse más allá del dominio de origen. Idealmente, desde el punto de vista de la seguridad, los filtros sólo permiten grupos conocidos (y potencialmente remitentes) y deniegan a los remitentes o grupos desconocidos.

Normalmente no es posible enumerar explícitamente todos los remitentes o grupos permitidos. se recomienda utilizar el filtro de configuración predeterminado para dominios PIM-SM con un único RP para cada grupo (sin grupo de malla MSDP):

```
!--- 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 !
```

Se recomienda filtrar de la forma más estricta posible, y en ambas direcciones, entrante y saliente.

Utilice para obtener más información sobre las recomendaciones de filtros SA de MSDP: https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) Limitación del Estado de MSDP

Cuando MSDP se habilita entre varios sistemas autónomos (AS), se recomienda limitar la cantidad de estado que se genera en el router debido a los mensajes "Source-Active" (SA) recibidos de los vecinos. Puede utilizar el comando **ip msdp sa-limit**:

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

Figura 14: Plano de control MSDP

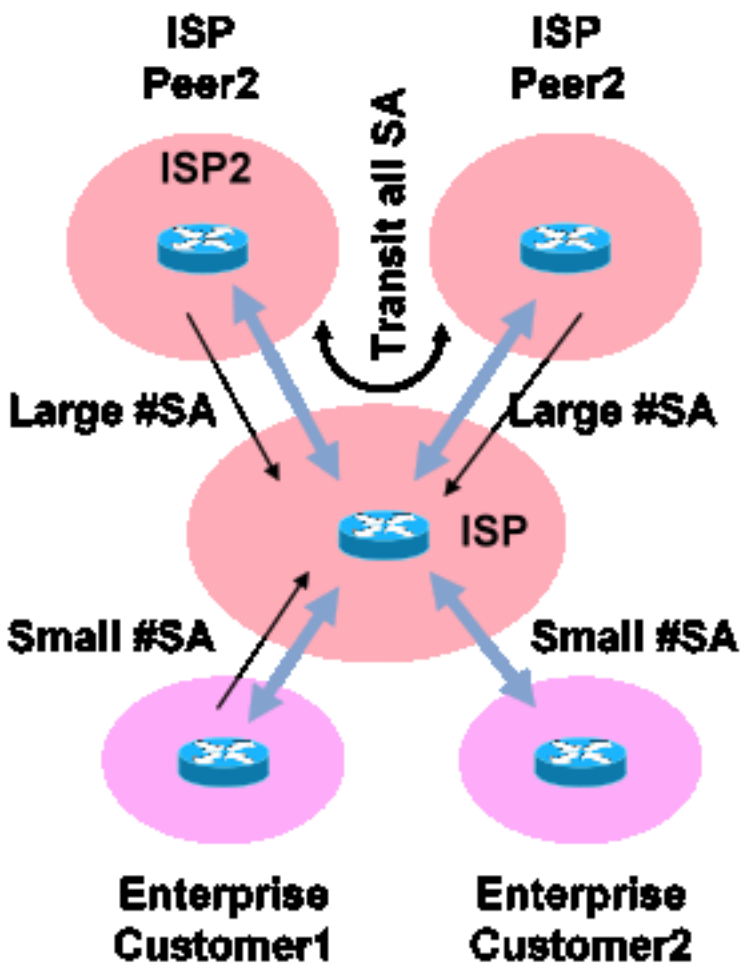

Fig14_MSDP_ControlPlane

Con el comando **ip msdp sa-limit** puede limitar el número de estados SA creados debido a mensajes SA aceptados de un peer MSDP. Entre las sencillas recomendaciones generales se incluyen las siguientes:

- Límite pequeño de Stub-neighbor
- Límite grande del vecino de tránsito (por ejemplo, #SAs máximo en Internet)
- ISP de tránsito: configure el número máximo de #SAs que admita su plataforma

3) Autenticación de vecino MD5 MSDP

Se recomienda utilizar la autenticación de contraseña del algoritmo Message-Digest (MD5) en los pares MSDP. Utiliza la opción de firma MD5 de TCP, equivalente al uso descrito en RFC 6691 para proteger BGP.

Figura 15: Autenticación de Vecino MD5 MSDP

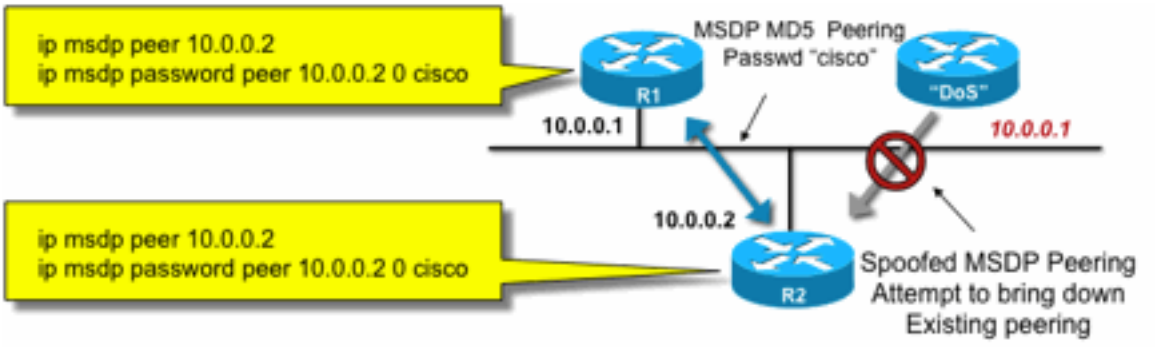

Fig15_MSDP_MD5Auth

Estas tres recomendaciones de seguridad de MSDP persiguen objetivos diferentes:

- La autenticación de vecino (con MD5) garantiza que sólo los pares MSDP de confianza puedan enviar mensajes.
- Los filtros SA garantizan que incluso un peer MSDP confiable sólo puede enviar anuncios SA que estén en línea con la política de grupo/origen previamente acordada.
- El límite de SA garantiza además que incluso con los anuncios legítimos (S,G) de pares legítimos, la memoria disponible no se puede agotar.

Problemas de remitente/origen

Muchos problemas de seguridad de multidifusión que se originan en el remitente se pueden mitigar con los mecanismos de seguridad de unidifusión adecuados. A continuación se recomiendan una serie de mecanismos de seguridad de unidifusión:

- **Protección contra suplantación de dirección de origen** (Unicast Reverse Path Forwarding, uRPF o ACL y protector de origen IP para la capa de acceso)
- **ACL de infraestructura** (deny ip any (to) <core address space>)

Estas medidas pueden utilizarse para bloquear ataques dirigidos contra el núcleo. Esto, por ejemplo, también resolvería problemas como ataques que utilizan paquetes de unidifusión PIM al RP, que está "dentro" de la red y, por lo tanto, estaría protegido por la ACL de infraestructura.

Control de acceso basado en filtros de paquetes: fuentes de control

En el ejemplo que se muestra en la figura 16, el filtro se configura en la interfaz LAN (E0) del router de multidifusión de primer salto (router designado). El filtro se define mediante una lista de control de acceso ampliada denominada "source". Esta ACL se aplica a la interfaz de origen del router designado conectado a la LAN de origen. De hecho, debido a la naturaleza del tráfico de multidifusión, podría ser necesario configurar un filtro similar en todas las interfaces de cara a la LAN en las que los orígenes podrían activarse. Dado que en todos los casos no es posible saber exactamente dónde se produce la actividad de origen, se recomienda aplicar estos filtros en todos los puntos de entrada a la red.

Figura 16: Orígenes de control

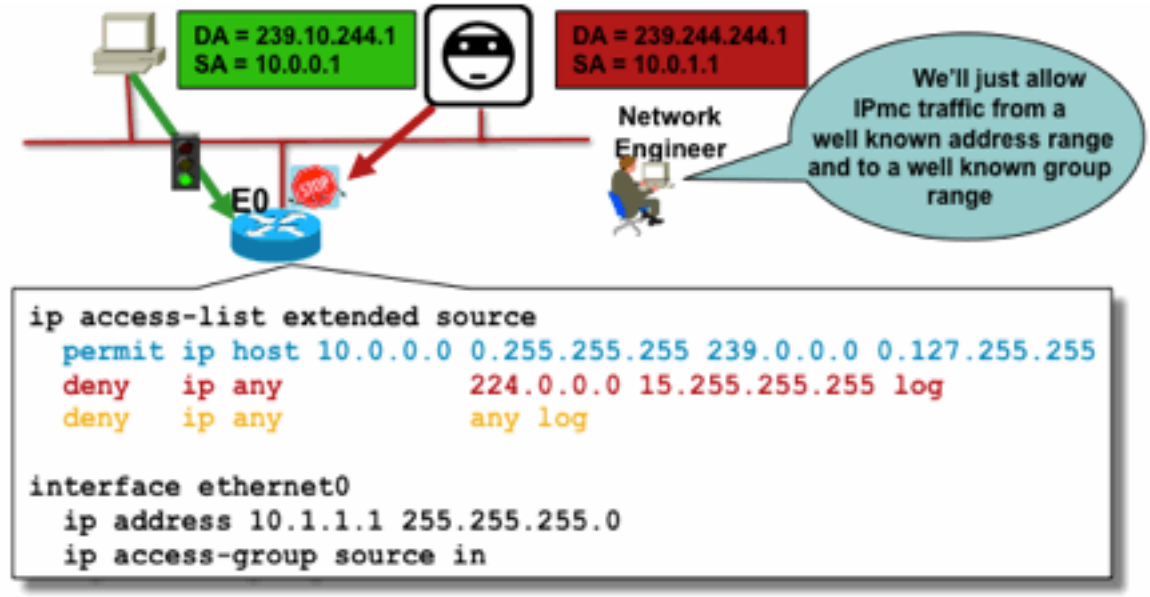

Fig16_Control_de_fuentes

El propósito de este filtro es evitar el tráfico de un origen o rango específico de direcciones de origen a un grupo o rango específico de direcciones de grupo. Este filtro actúa antes de que PIM cree rutas multicast y ayuda a limitar el estado.

Se trata de una ACL de plano de datos estándar. Esto se implementa en los ASIC en las plataformas de gama alta y no se produce ninguna penalización en el rendimiento. Se recomiendan y prefieren las ACL del plano de datos en lugar del plano de control para los orígenes conectados directamente, ya que minimizan el impacto del plano de control del tráfico no deseado. También es muy eficaz limitar el destino (direcciones de grupo de multidifusión IP) al que se pueden enviar paquetes. Dado que se trata de un comando de router, no puede superar una dirección IP de origen falsificada (consulte la parte anterior de esta sección). Por lo tanto, se recomienda proporcionar mecanismos de capa 2 (L2) adicionales o una política uniforme para todos los dispositivos que se puedan conectar a una red de área local concreta/red de área local virtual (LAN/VLAN).

> **Nota:** La palabra clave "log" en una ACL es muy útil para comprender los resultados de una entrada ACL específica; sin embargo, esto consume recursos de la CPU y debe manejarse con cuidado. Además, en las plataformas basadas en hardware, los mensajes de registro de ACL son producidos por una CPU y, por lo tanto, se debe considerar el impacto de la CPU.

Control de código fuente PIM-SM

Una de las ventajas reales de la arquitectura ASM/PIM-SM desde el punto de vista de la seguridad es el hecho de que el punto de encuentro proporciona un único punto de control para todas las fuentes de la red para cualquier rango de grupos. Esto se puede aprovechar con un dispositivo denominado filtro accept-register. El comando para este filtro es el siguiente:

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

Figura 17: Control de código fuente PIM-SM

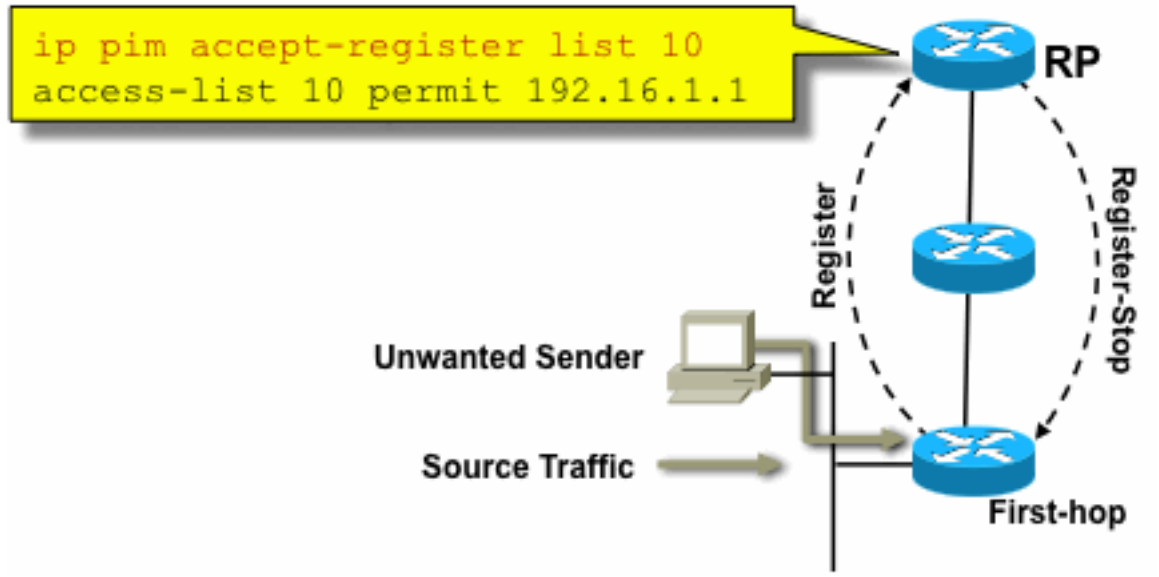

Fig17_PIMSM_Control

En una red PIM-SM, un origen de tráfico no deseado se puede controlar con este comando. Cuando el tráfico de origen llega al router de primer salto, el router de primer salto (DR) crea el estado (S,G) y envía un mensaje de registro de origen PIM al RP. Si el origen no aparece en la lista de filtros de aceptación-registro (configurada en el RP), el RP rechaza el registro y devuelve un mensaje de registro-detención inmediato al DR.

En el ejemplo mostrado, se ha aplicado una ACL simple al RP, que filtra solamente en la dirección de origen. También es posible filtrar el origen Y el grupo con el uso de una ACL extendida en el RP.

Hay inconvenientes con los filtros de origen porque con el comando **pim accept-register** en el RP, el estado PIM-SM (S,G) todavía se crea en el router de primer salto del origen. Esto puede resultar en tráfico en los receptores locales al origen y ubicados entre el origen y el RP. Además, el comando **pim accept-register** funciona en el plano de control del RP. Esto podría usarse para sobrecargar el RP con mensajes de registro falsos y posiblemente causar una condición de DoS.

Se recomienda aplicar el comando pim accept-register en el RP además de otros métodos, como la aplicación de ACL de plano de datos simples en todos los DR, en todos los puntos de ingreso a la red. Aunque las ACL de ingreso en el DR serían suficientes en una red perfectamente configurada y operada, se recomienda configurar el comando **pim accept-register** en el RP como mecanismo de seguridad secundario en caso de configuraciones erróneas en los routers de borde. Los mecanismos de seguridad por capas con el mismo objetivo se denominan "defensa en profundidad" y son un principio de diseño común en materia de seguridad.

Problemas del Receptor - Control de IGMP/MLD

La mayoría de los problemas del receptor caen en el dominio de las interacciones del protocolo del receptor IGMP/MLD.

Figura 18: Control de IGMP

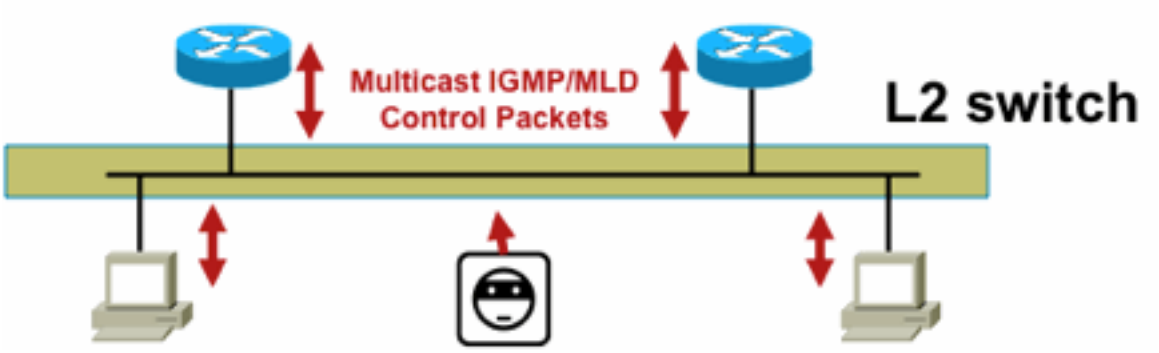

Fig18_Control_IGMP

Cuando se filtran paquetes IGMP o MLD, recuerde estos puntos:

- IPv4: IGMP es un tipo de protocolo IPv4 (protocolo IPv4 2)
- IPv6: MLD se transporta en paquetes de tipo de protocolo ICMPv6

El proceso IGMP se habilita de forma predeterminada en cuanto se habilita la multidifusión IP. Los paquetes IGMP también transportan estos protocolos y, por lo tanto, todos estos protocolos se habilitan cada vez que se habilita la multidifusión:

- PIMv1: PIMv1 fue la primera versión de PIM y siempre está habilitado en Cisco IOS para la migración. Todas las implementaciones actuales utilizan PIMv2.
- Mrinfo - Mrinfo es un comando Unix que Cisco IOS heredó para mostrar los vecinos multicast. Cisco recomienda el uso de SNMP en lugar del comando mrinfo.
- DVMRP: DVMRP es un protocolo de vector de distancia de modo denso heredado con características de ampliación muy limitadas. El soporte del IOS de Cisco para DVMRP se ha retirado o ya está obsoleto.
- Mtrace: Mtrace es el equivalente multidifusión de unicast "traceroute" y es una herramienta útil

Para obtener más información, vea Números de tipo del protocolo de administración de grupos de Internet (IGMP) de 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
```

Los paquetes de IGMP unidifusión (para IGMP/UDLR) se pueden filtrar, ya que son los paquetes de ataque más probables y los paquetes de protocolo IGMP no válidos. Cisco IOS admite paquetes IGMP unidifusión para admitir enlaces unidireccionales y otras condiciones de excepción.

Los paquetes de consulta IGMP/MLD falsificados pueden dar como resultado una versión de IGMP inferior a la esperada.

En particular, lo ideal es que los hosts nunca envíen consultas IGMP porque una consulta enviada con una versión de IGMP inferior puede hacer que todos los hosts que reciban esta consulta vuelvan a la versión inferior. En presencia de hosts IGMPv3 / SSM, esto puede "atacar" los flujos SSM. En el caso de IGMPv2, esto puede resultar en latencias de licencia más largas.

Si una LAN no redundante con un único solicitante IGMP está presente, el router necesita descartar las consultas IGMP recibidas.

Si existe una LAN pasiva redundante/común, se requiere un switch capaz de indagación IGMP. Hay 2 características específicas que pueden ayudar en este caso:

- Protección del router
- comando Versión mínima de IGMP

Protección del router

Cualquier puerto de switch puede convertirse en un puerto de router multicast si el switch recibe un paquete de control de router multicast (consulta general IGMP, saludo PIM o saludo CGMP) en ese puerto. Cuando un puerto de switch se convierte en un puerto de router multicast, todo el tráfico multicast se envía a ese puerto. Esto se puede evitar con "Router Guard". La función Router Guard no requiere que se active la indagación IGMP.

La función Router Guard permite que un puerto especificado sea designado como puerto de host multicast. El puerto no puede convertirse en un puerto del router, incluso si se reciben paquetes de control del router multicast.

Estos tipos de paquetes se descartan si se reciben en un puerto que tiene activado Router Guard:

- Mensajes de consulta IGMP
- Mensajes IPv4 PIMv2
- Mensajes IGMP PIM (PIMv1)
- Mensajes IGMP DVMRP
- Mensajes del protocolo de administración de grupos (RGMP) de puertos del router
- Mensajes del protocolo de administración de grupos de Cisco (CGMP)

Cuando se descartan estos paquetes, se actualizan las estadísticas que indican que los paquetes se descartan debido a la protección del router.

Versión mínima de IGMP

Es posible configurar la versión mínima de hosts IGMP permitidos. Por ejemplo, puede no permitir todos los hosts IGMPv1 o todos los hosts IGMPv1 e IGMPv2. Este filtro sólo se aplica a los informes de pertenencia.

Si los hosts están conectados a una LAN "pasiva" común (por ejemplo, un switch que no soporta IGMP Snooping, o que no está configurado para ello), tampoco hay nada que un router pueda hacer acerca de tales consultas falsas que no sea ignorar los informes de membresía de la "versión anterior" que luego se activan, y no recurrir a sí mismo.

Dado que las consultas IGMP deben ser visibles para todos los hosts, no es posible utilizar un mecanismo de autenticación de mensajes basada en hash (HMAC) con una clave previamente compartida, como IPSec de clave estática, para autenticar consultas IGMP desde "routers válidos". Si dos o más routers están conectados a un segmento LAN común, se requiere una elección de solicitante IGMP. En ese caso, el único filtro que se podría utilizar es un filtro de grupo

de acceso IP basado en la dirección IP de origen del otro router IGMP que envía consultas.

Se deben permitir los paquetes IGMP de multidifusión "normales".

Este filtro se puede utilizar en los puertos del receptor para permitir solamente los paquetes IGMP "buenos", y para filtrar los paquetes "malos" conocidos:

```
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
```

> **Nota:** Este tipo de filtro IGMP se puede utilizar en ACL de recepción o CoPP. En ambas aplicaciones, debe combinarse con filtros para otro tráfico gestionado, como protocolos de plano de administración y routing.

Figura 19: Control de acceso del receptor del host

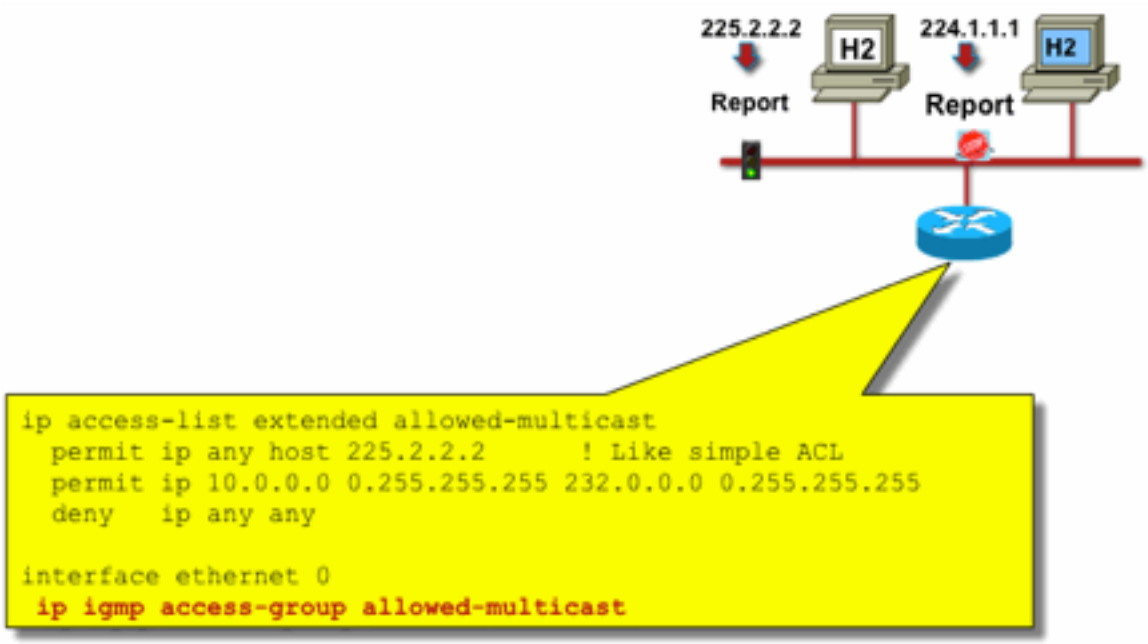

Fig19_Host_Receiver_Access

Para filtrar el tráfico a un receptor, no filtre el tráfico del plano de datos, sino el protocolo IGMP del plano de control. Dado que IGMP es un requisito previo necesario para recibir tráfico de multidifusión, no se requieren filtros de plano de datos.

En particular, puede restringir los flujos de multidifusión a los que pueden unirse los receptores (conectados a la interfaz en la que está configurado el comando). En este caso, utilice el comando **ip igmp access-group / ipv6 mld access-group**:

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

Para los grupos de ASM, este comando sólo filtra según la dirección de destino. A continuación, se ignora la dirección IP de origen en la ACL. Para los grupos SSM que utilizan IGMPv3 / MLDv2, filtra en la IP de origen y de destino.

Este ejemplo filtra un grupo determinado para todos los altavoces IGMP:

```
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
```

Este ejemplo filtra altavoces IGMP específicos (por lo tanto, receptores multicast específicos) para un grupo determinado:

```
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
```

Nota: Recuerde que para los grupos de ASM se ignora el origen.

Control de admisión

El control de acceso proporciona una respuesta binaria, sí o no para ciertos flujos, independientemente del estado de la red. El control de admisión por contraste limita el número de recursos que un emisor / receptor puede utilizar, asumiendo que pasaron los mecanismos de control de acceso. Hay varios dispositivos disponibles para ayudar con el control de admisión en un entorno multicast.

Límites IGMP globales y por interfaz

En el router más cercano a los receptores de multidifusión interesados, existe la posibilidad de limitar el número de grupos IGMP unidos tanto globalmente como por interfaz. Puede utilizar los comandos **ip igmp limit/ipv6 mld limit**:

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

Se recomienda que este límite se configure siempre por interfaz y también globalmente. En cada caso, el límite se refiere a los recuentos de entradas en la memoria caché IGMP.

Los dos ejemplos siguientes muestran cómo se puede utilizar este comando para ayudar a limitar el número de grupos en el borde de una red de banda ancha residencial.

Ejemplo 1: restringir los grupos recibidos a solo los anuncios de SDR más un canal recibido

El directorio de sesión (SDR) actúa como guía de canales para algunos receptores de multidifusión. Consulte RFC 2327 para obtener más detalles.

Un requisito común es restringir los receptores para recibir el grupo SD más un canal. Este ejemplo de configuración se puede utilizar:

```
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
```

La lista de acceso de este ejemplo especifica sólo la guía de canales; el comando global **ip igmp limit** limita cada fuente IGMP a un solo (1) canal, pero no incluye la guía de canales, que siempre se puede recibir. El comando interface invalida el comando global y permite que se reciban dos (2) canales, además de la guía de canales, en esta interfaz.

Ejemplo 2 - Control de admisión en el link DSLAM de agregación

Este comando también se puede utilizar para proporcionar una forma de control de admisión de ancho de banda. Por ejemplo, si fuera necesario distribuir 300 canales de SDTV, que son de 4 Mbps cada uno, y hubiera un enlace de 1 Gbps al multiplexor de acceso de línea de suscriptor digital (DSLAM), puede tomar la decisión de una política para limitar el ancho de banda de TV a 500 Mbps y dejar el resto para Internet y otros usos. En ese caso, puede limitar los estados IGMP a 500 Mbps/4 Mbps = 125 estados IGMP.

Esta configuración se puede utilizar en este caso:

Figura 20: Uso de límites IGMP por interfaz; Control de admisión en enlace Agg-DSLAM

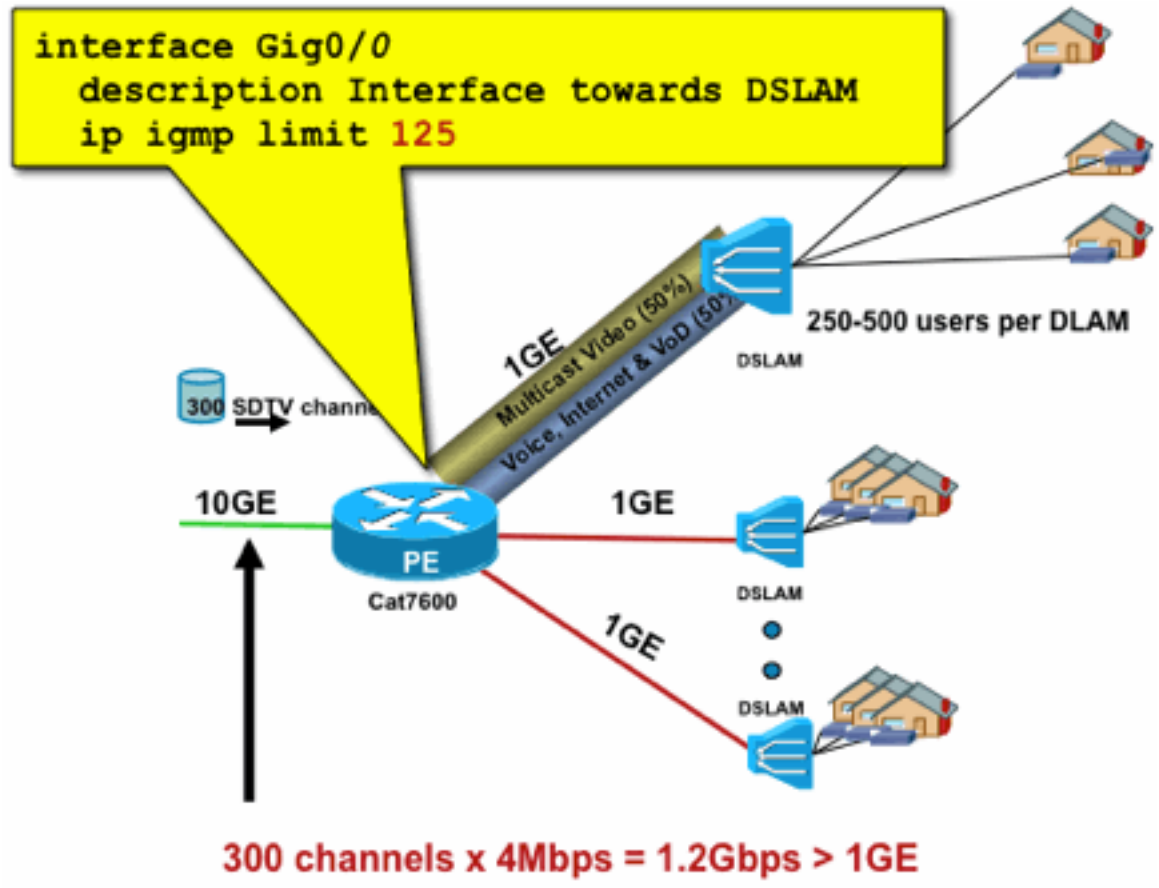

Fig20_PerInterface_IGMP

Límites de ruta multicast por interfaz

La habilitación de los límites de estado de ruta multicast por interfaz es una forma más genérica de control de admisión. No solo limita el estado de IGMP y PIM en una interfaz saliente, sino que también proporciona una forma de límites de estado en las interfaces entrantes.

Utilice el comando **ip multicast limit**:

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

El estado se puede limitar por separado en las interfaces de entrada y salida. El estado de origen conectado directamente también se puede limitar con el uso de la palabra clave "conectado". Los ejemplos ilustran el uso de este comando:

Ejemplo 1 - Control de admisión de salida en enlace Agg-DSLAM

En este ejemplo, hay 300 canales de TV SD. Supongamos que cada canal SD necesita 4 Mbps, con un total de no más de 500 Mbps. Por último, suponga también que necesita compatibilidad con los paquetes Basic, Extended y Premium. Ejemplo de asignaciones de ancho de banda:

- 60% / 300 Mbps básico
- 20% / 100 Mbps ampliado
- Premium de 20%/100 Mbps

A continuación, utilice 4 Mbps por canal y limite el enlace ascendente DSLAM a:

- Básico 75 estados
- 25 estados ampliados
- Premium 25 estados

Configure el límite en la interfaz saliente que enfrenta el DSLAM desde el PEAgg:

Figura 21: Uso de límites de ruta multicast por interfaz; Control de admisión en enlace Agg-DSLAM

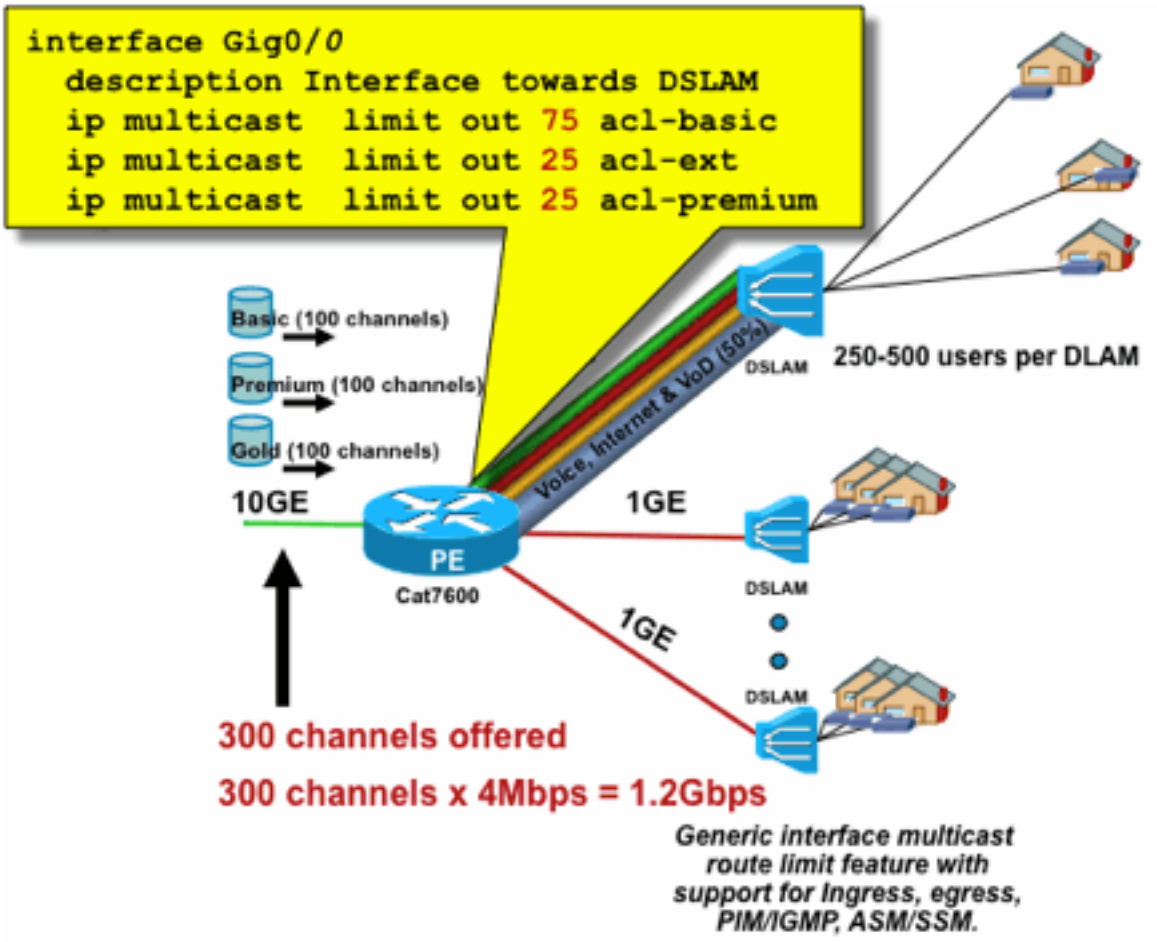

Fig21_PerInterface_Mroute

Ejemplo 2 - Control de admisión de ingreso en el link Agg-DSLAM

En lugar del límite "out" en la interfaz saliente del dispositivo ascendente, es posible utilizar límites RPF en la interfaz RPF del dispositivo descendente. Esto efectivamente tiene el mismo resultado que el ejemplo anterior, y podría ser útil si el dispositivo de flujo descendente no es un dispositivo Cisco IOS.

Figura 22: Uso de límites de ruta multicast por interfaz; Control de admisión de entrada

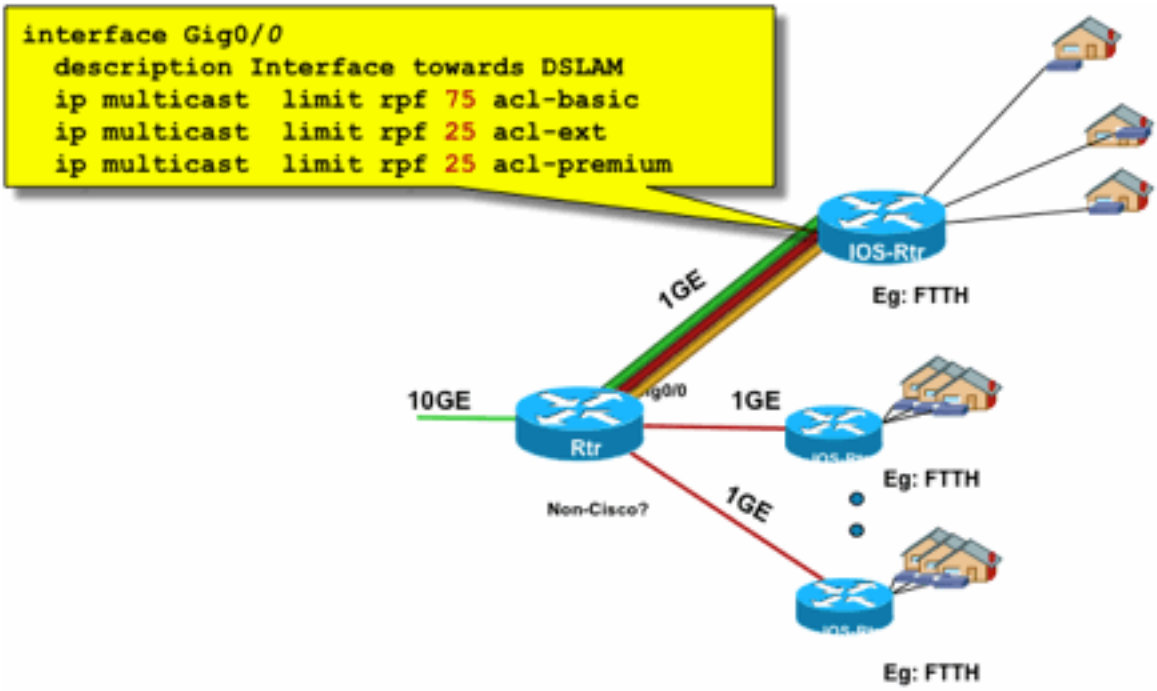

Fig22_PerInterface_Mroute_inputControl

Ejemplo 3: límites basados en ancho de banda

Puede hacer una subdivisión adicional del ancho de banda de acceso entre varios proveedores de contenido y ofrecer a cada proveedor de contenido una porción justa del ancho de banda en el link ascendente al DSLAM. En ese caso, utilice el **comando ip multicast limit cost**:

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

Con este comando, es posible atribuir un "costo" (utilice el valor especificado en "multiplicador") a cualquier estado que coincida con la ACL extendida en el límite de multidifusión IP.

Este comando es un comando global y se pueden configurar varios costes simultáneos.

En este ejemplo, es necesario admitir tres proveedores de contenido diferentes con un acceso justo a cada uno de ellos en la red. Además, en este ejemplo es necesario admitir secuencias de MPEG (Moving Picture Experts Group) de varios tipos:

SDTV MPEG2: 4 Mbps
HDTV MPEG2: 18 Mbps
SDTV MPEG4: 1,6 Mbps
HDTV MPEG4: 6 Mbps

En tal caso, podría asignar los costos de ancho de banda a cada tipo de flujo y compartir el resto de los 750 Mbps entre los tres proveedores de contenido con esta configuración:

```
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
```

Figura 23: Factor de Costo para los Límites de Estado de Ruta Multicast por Interfaz

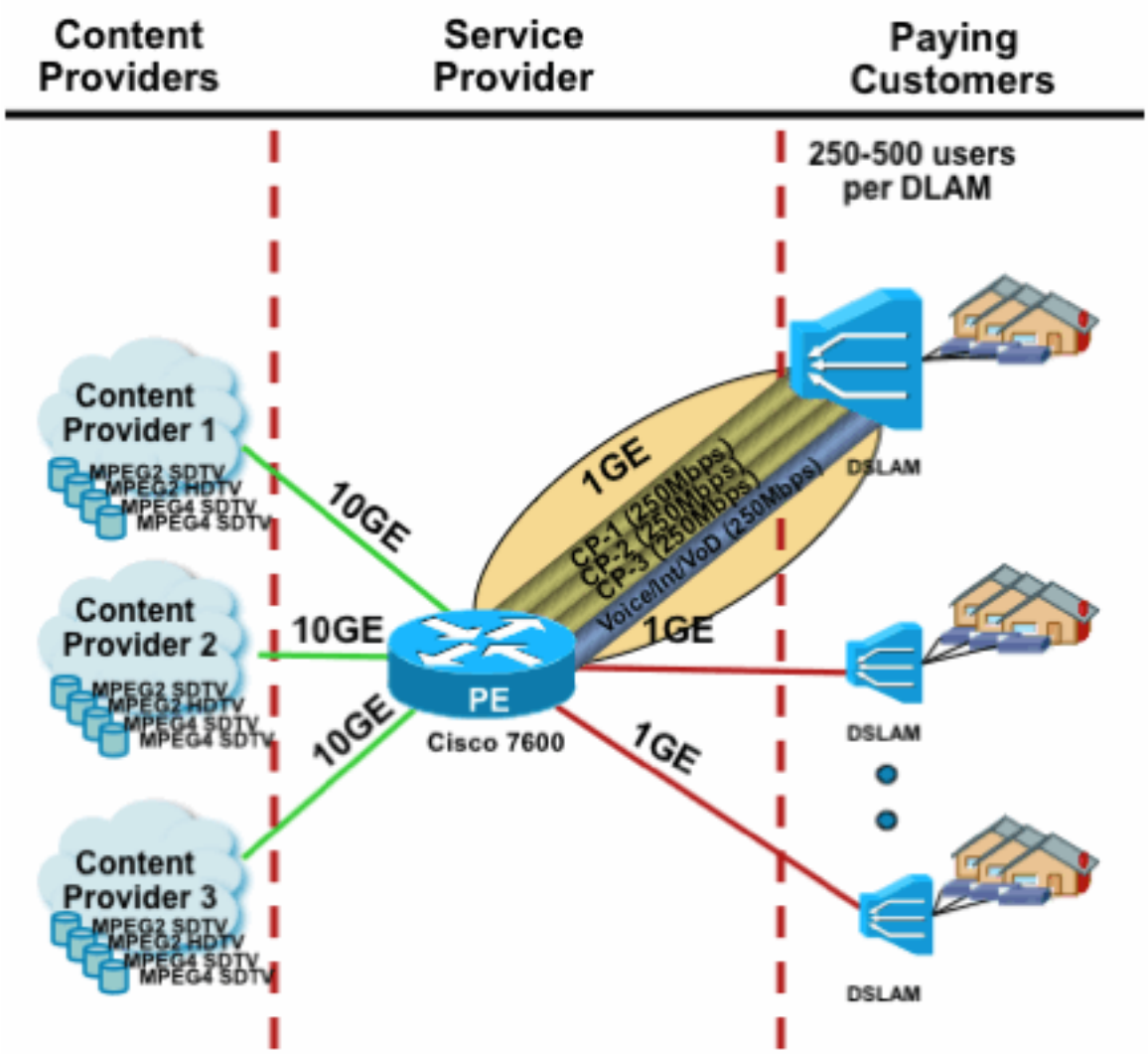

Fig23_Cost_P

erInterface

Multidifusión e IPSec

Introducción a GET VPN

Al igual que con la unidifusión, el tráfico de multidifusión a veces también debe protegerse para proporcionar confidencialidad o protección de integridad. Hay dos esferas principales en las que podrían requerirse esos servicios:

- Cifrado de secuencias de multidifusión (por ejemplo, en aplicaciones bancarias que transmiten datos confidenciales a un gran conjunto de receptores que utilizan multidifusión): se trata de la seguridad del plano de datos.
- Cifrado de protocolos del plano de control que utilizan multidifusión, OSPF o PIM, por ejemplo: se trata de la seguridad del plano de control.

IPSec como protocolo [RFC 6040, 7619, 4302, 4303, 5282] se limita específicamente al tráfico unidifusión (mediante RFC). Allí, se establece una "asociación de seguridad" (SA) entre dos pares

de unidifusión. Para aplicar IPSec al tráfico de multidifusión, una opción es encapsular el tráfico de multidifusión dentro de un túnel GRE y, a continuación, aplicar IPSec al túnel GRE, que es unidifusión. Un enfoque más reciente utiliza una única asociación de seguridad establecida entre todos los miembros del grupo. El dominio de interpretación de grupo (GDOI) [RFC 6407] define cómo se consigue.

Basándose en GDOI, Cisco desarrolló una tecnología denominada VPN de transporte de cifrado de grupo (GET). Esta tecnología utiliza "Tunnel Mode with Address Preservation", tal y como se define en el documento "draft-ietf-msec-ipsec-extensions". En GET VPN, primero se establece una asociación de seguridad de grupo entre todos los miembros del grupo. Posteriormente, el tráfico se protege, ya sea con ESP (carga de seguridad encapsulada) o AH (encabezado de autenticación), que utiliza el modo de túnel con preservación de direcciones.

En resumen, GET VPN encapsula un paquete de multidifusión que utiliza la información de dirección del encabezado original y, a continuación, protege el paquete interno en relación con la directiva de grupo, por ejemplo, con un ESP.

La ventaja de GET VPN es que el tráfico multicast no se ve afectado en absoluto por los mecanismos de encapsulación de seguridad. Las direcciones de encabezado IP enrutadas siguen siendo las mismas que el encabezado IP original. El tráfico multidifusión se puede proteger de la misma manera con o sin GET VPN.

La política que se aplica a los nodos GET VPN se define centralmente en un servidor de clave de grupo y se distribuye a todos los nodos de grupo. Por lo tanto, todos los nodos de grupo tienen la misma política y la misma configuración de seguridad aplicada al tráfico de grupo. De manera similar a IPSec estándar, la política de cifrado define qué tipo de tráfico debe protegerse de qué manera. Esto permite utilizar GET VPN para diversos fines.

Utilice GET VPN para cifrar el tráfico del plano de datos multidifusión

La política de cifrado de toda la red se establece en el servidor de claves de grupo y se distribuye a los terminales GET VPN. La directiva contiene la directiva IPSec (modo IPSec): modo de túnel con conservación de encabezados) y los algoritmos de seguridad que se deben utilizar (por ejemplo, AES). También contiene una política que describe qué tráfico se puede asegurar, según lo definido por una ACL.

VPN GET se puede utilizar para tráfico de multidifusión y unidifusión. Una ACL podría definir una política para asegurar el tráfico de unidifusión:

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

Esto cifraría todo el tráfico con una IP de origen de 10/8 y una IP de destino de 10/8. El resto del tráfico, por ejemplo, el tráfico de 10/8 a otra dirección, sería ignorado por GET VPN.

La aplicación de GET VPN para el tráfico multicast es técnicamente la misma. Por ejemplo, esta entrada de control de acceso (ACE) se puede utilizar para proteger el tráfico desde cualquier origen a los grupos de multidifusión respectivos:

```
permit ip any 239.192.0.0 0.0.255.255
```

Esta directiva coincide con todos los orígenes ("cualquiera") y todos los grupos de multidifusión

que comienzan por 239.192. El tráfico a otros grupos de multidifusión no está protegido.

> **Nota:** Se debe prestar gran atención a la construcción de la ACL criptográfica. El tráfico de administración, o el tráfico que se origina fuera del dominio GET VPN pero termina dentro (es decir, el tráfico que pasa solamente un punto final de cifrado), debe excluirse de la política GDOI.

Los errores comunes incluyen:

- permit ip any 224.0.0.0 0.255.255.255: Esto también cifra el tráfico OSPF y otro tráfico del plano de control, que está destinado a un router par, por ejemplo.
- El tráfico de administración no se excluye de la política de cifrado, que termina dentro de la red. Esto incluye el propio tráfico GDOI.

Utilice GET VPN para autenticar el tráfico del plano de control

Por lo general, se recomienda autenticar el tráfico del plano de control, como los protocolos de enrutamiento, para asegurarse de que los mensajes proceden de un par de confianza. Esto es comparativamente simple para los protocolos del plano de control que utilizan unicast, como BGP. Sin embargo, muchos protocolos del plano de control utilizan tráfico multidifusión. Algunos ejemplos son OSPF, RIP y PIM. Consulte Registro de Espacio de Direcciones Multicast IPv4 de IANA para obtener la lista completa.

Algunos de estos protocolos tienen autenticación integrada, como el protocolo de información de enrutamiento (RIP) o el protocolo de enrutamiento de grupo interior mejorado (EIGRP); otros se basan en IPSec para proporcionar esta autenticación (por ejemplo, OSPFv3 o PIM). Para este último caso, GET VPN proporciona una forma escalable de proteger estos protocolos. En la mayoría de los casos, el requisito es la autenticación de mensajes de protocolo o, en otras palabras, la verificación de que un mensaje fue enviado por un peer de confianza. Sin embargo, GET VPN también permite el cifrado de dichos mensajes.

Para proteger (normalmente autenticar solo) dicho tráfico del plano de control, el tráfico debe describirse con una ACL e incluirse en la política GET VPN. Los detalles dependen del protocolo que se va a asegurar, donde se debe prestar atención a si la ACL incluye tráfico que pasa solamente un nodo GET VPN de ingreso (que está encapsulado), o también un nodo de egreso.

Existen dos formas fundamentales de proteger los protocolos PIM:

- **permit ip any 224.0.0.13 0.0.0.0**: Este es el grupo de multidifusión "Todos los routers PIM". Sin embargo, esto no protege los mensajes PIM de unidifusión
- **permit pim any any**: Esto protege el protocolo PIM, independientemente de si se utiliza multidifusión o unidifusión

> **Nota:** Los comandos se proporcionan como ejemplos para ayudar a explicar un concepto. Por ejemplo, es necesario excluir ciertos protocolos PIM utilizados para arrancar PIM, como BSR o Auto-RP. Ninguno de los métodos tiene ciertas ventajas e inconvenientes que dependen de la implementación. Consulte la documentación específica sobre cómo proteger PIM con GET VPN para obtener más información.

Conclusiones

La multidifusión es un servicio cada vez más habitual en las redes. La aparición de los servicios IPTV en las redes de banda ancha residenciales/domésticas y el avance hacia las aplicaciones de comercio electrónico en muchos de los mercados financieros mundiales son solo dos ejemplos de requisitos que convierten a la multidifusión en un requisito absoluto. La multidifusión conlleva una serie de retos de configuración, funcionamiento y gestión diferentes. Uno de los retos clave es la seguridad.

Este documento examinó una variedad de maneras en las que se puede asegurar la multidifusión:

- En primer lugar, observe los planos de datos y control de multidifusión generales, una explicación de cómo las diferencias con respecto a la unidifusión presentan nuevos retos de seguridad.
- A continuación, se examinó con cierto detalle un examen de los protocolos clave que se encuentran en una red multidifusión, en particular IGMP, PIM y MSDP. En cada caso, se proporcionó una descripción de las amenazas de seguridad y las prácticas recomendadas para mitigar estas amenazas.
- Además, hay algunos ejemplos concretos de cómo la multidifusión puede protegerse en algunas aplicaciones específicas, como las redes periféricas de banda ancha, donde el ancho de banda puede ser limitado en comparación con la cantidad de ancho de banda que podrían requerir flujos de vídeo específicos.
- Por último, la arquitectura GET VPN se describió como un medio de multidifusión integrada con IPSec para proporcionar VPN seguras.

Con la seguridad de multidifusión en mente, recuerde lo diferente que es la unidifusión. La transmisión de multidifusión se basa en la creación del estado dinámico, la multidifusión implica la replicación dinámica de paquetes y la multidifusión crea árboles unidireccionales en respuesta a los mensajes PIM JOIN/PRUNE. La seguridad de todo este entorno implica la comprensión e implementación de un marco completo de comandos de Cisco IOS. Estos comandos se centran principalmente en la protección de operaciones de protocolo, estados (multidifusión) o reguladores de tráfico colocados contra paquetes como CoPP. Con el uso correcto de estos comandos es posible proporcionar un servicio protegido robusto para multidifusión IP.

En resumen, hay varios enfoques que se promueven y se describen en este documento:

1. Uso generalizado de SSM: este es el modo PIM más sencillo que también permite el uso de reenvío (S,G).
2. Si se necesitan servicios de ASM, asegúrese de que se puede proporcionar un servicio sólido; el uso de RP definidos estáticamente proporciona un plano de control más seguro que los anuncios de RP dinámicos. Auto-RP y BSR son más flexibles
3. Si PIM-SM está habilitado, observe las áreas de vulnerabilidad particular, como el túnel de registro al RP, y asegúrese de que el DR esté siempre bien protegido. CoPP es muy útil en estas áreas.
4. Si se necesitan servicios de ASM entre dominios, considere si se puede implementar BiDir PIM.
5. Utilice límites de estado de ruta multicast/igmp globales: comprenda las capacidades de sus plataformas junto con la cantidad máxima de estado esperada que necesita en circunstancias normales y en el peor de los casos. Configure límites dentro de las capacidades de su plataforma que permitan que su red funcione al máximo.
6. Filtros fundamentales: rACL/CoPP y ACL de infraestructura, que bloquean PIM en la capa de acceso

La multidifusión IP es un medio interesante y escalable para ofrecer una variedad de servicios de aplicaciones. Al igual que la unidifusión, debe protegerse en diversas áreas. Este documento proporciona los bloques de creación básicos que se pueden utilizar para proteger una red de multidifusión IP.

Información Relacionada

- Pautas para la Asignación de Direcciones IP Multicast Empresariales
- Configurar filtros IGMP de IPv4
- VPN con transporte cifrado de grupo

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).