218004-secure-ip-multicast-deployments

Contents

Introdução

Este documento descreve orientações gerais sobre as melhores práticas para proteger uma infraestrutura de rede multicast IP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo IP Multicast

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento abrange alguns conceitos básicos, terminologia e discute os tópicos listados:

- Mecanismos para proteger uma plataforma específica e a rede em geral.
- Qualquer modelo Source Multicast (ASM) e Source Specific Multicast (SSM).
- Segurança de Rede Virtual Privada (MVPN - Virtual Private Network) multicast.
- Arquitetura de Rede Virtual Privada (VPN - Virtual Private Network) GET (Transporte

Criptografado de Grupos) que fornece confidencialidade e integridade para plano de dados multicast ou tráfego de plano de controle.

Terminologia

No multicast IP, há dois modelos de serviço clássicos:

1. Qualquer Multicast de Origem (ASM)
2. Multicast Específico de Origem (SSM)

No ASM, o receptor ingressa em um grupo G por meio de um relatório de associação Internet Group Membership Protocol (IGMP) ou Multicast Listener Discovery (MLD) para indicar o grupo. Esse relatório solicita o tráfego enviado por qualquer origem para o grupo G e, portanto, o nome "qualquer origem". Por outro lado, no SSM, o receptor se junta a um canal específico definido por uma fonte S, que envia para um grupo G. Cada um desses modelos de serviço é descrito em detalhes abaixo.

Multicast de qualquer origem

O modelo ASM é caracterizado por duas classes de protocolo: "flood-and-prune de modo denso" e "sparse mode explicit join":

i) Protocolos de Inundação e Remoção de Modo Denso (DVMRP / MOSPF / PIM-DM)

Em protocolos de modo denso, todos os roteadores na rede estão cientes de todas as árvores, suas fontes e receptores. Protocolos como o Distance Vetor Multicast Routing Protocol (DVMRP) e o modo denso Protocol Independent Multicast (PIM) inundam informações de "fonte ativa" em toda a rede e criam árvores por meio da criação do "Prune State" em partes da topologia em que o tráfego para uma árvore específica é indesejado. Eles também são chamados de protocolos flood-and-prune. No Multicast Open Shortest Path First (MOSPF), as informações sobre receptores são inundadas em toda a rede para suportar a criação de árvores.

Os protocolos do modo denso são indesejáveis porque cada árvore construída em alguma parte da rede pode sempre causar a utilização de recursos (com impacto de convergência) em todos os roteadores da rede (ou dentro do escopo administrativo, se configurado). Esses protocolos não serão discutidos mais no restante deste artigo.

ii) Protocolos de Junção Explícita de Modo Esparso (PIM-SM/PIM-BiDir)

Com protocolos de junção explícita de modo esparso, os dispositivos não criam um estado específico de grupo na rede, a menos que um receptor tenha enviado um relatório de associação IGMP/MLD explícito (ou "junção") para um grupo. Essa variante do ASM é conhecida por escalar bem e é o paradigma de multicast do foco.

Essa é a base para o Modo PIM-Sparse, que a maioria das implantações de multicast já usou até agora. Essa também é a base para o PIM bidirecional (PIM-BiDir), que é cada vez mais

implantado para MUITAS (origens) para MUITAS (receptores) aplicações.

Esses protocolos são chamados de modo esparso porque suportam eficientemente árvores de entrega multicast IP com uma população de receptores "esparsa" e criam um estado de plano de controle apenas nos roteadores no caminho entre as fontes e os receptores e no PIM-SM/BiDir, o Ponto de Reunião (RP). Eles nunca criam um estado em outras partes da rede. O estado em um roteador só é construído explicitamente quando ele recebe uma junção de um roteador ou receptor downstream, daí o nome "protocolos explícitos de junção".

Tanto o PIM-SM quanto o PIM-BiDir empregam "ÁRVORES COMPARTILHADAS", que permitem que o tráfego de qualquer origem seja encaminhado a um receptor. O estado multicast em uma árvore compartilhada é conhecido como estado (*,G), onde * é um curinga para QUALQUER ORIGEM. Além disso, o PIM-SM suporta a criação de estado que se relaciona ao tráfego de uma origem específica. Elas são conhecidas como ÁRVORES DE ORIGEM, e o estado associado é conhecido como estado (S,G).

Multicast específico da origem

O SSM é o modelo usado quando o receptor (ou algum proxy) envia "junções" (S,G) para indicar que deseja receber o tráfego enviado pela origem S para o grupo G. Isso é possível com relatórios de associação do modo IGMPv3/MLDv2 "INCLUDE". Esse modelo é conhecido como o modelo Source-Specific Multicast (SSM). O SSM exige o uso de um protocolo de junção explícita entre roteadores. O protocolo padrão para isso é o PIM-SSM, que é simplesmente o subconjunto do PIM-SM usado para criar árvores (S,G). Não há árvores compartilhadas (*,G) no SSM.

Os receptores multicast podem, assim, "participar" de um grupo ASM G, ou "participar" (ou, mais precisamente, "inscrever-se") de um canal SSM (S,G). Para evitar a repetição do termo "grupo ASM ou canal SSM", o termo fluxo (multicast) é usado, o que implica que o fluxo poderia ser um grupo ASM ou um canal SSM.

Protocolos multicast/tipos de pacotes relevantes

Para proteger uma rede multicast, é importante entender os tipos de pacotes comumente encontrados e como se proteger contra eles. Há três protocolos principais que devem ser considerados:

1. IGMP/MLD
2. MIP
3. MSDP

Na próxima seção, cada um desses protocolos será discutido e os problemas que podem surgir com cada um deles, respectivamente.

Pacotes IGMP/MLD

IGMP / MLD é o protocolo usado pelos receptores multicast para sinalizar a um roteador que eles desejam receber conteúdo para um grupo multicast específico. O Internet Group Membership Protocol (IGMP) é o protocolo usado no IPv4 e o Multicast Listener Discovery (MLD) é o protocolo usado no IPv6.

Há duas versões do IGMP que são comumente implantadas, IGMPv2 e IGMPv3. Há também duas versões do MLD que são comumente implantadas, MLDv1 e MLDv2.

IGMPv2 e MLDv1 são funcionalmente equivalentes e IGMPv3 e MLDv2 são funcionalmente equivalentes.

Esses protocolos são especificados nestes links:

IGMPv2: RFC 2236

MLDv1: RFC 3590

IGMPv3 e MLDv2: RFC 4604

O IGMPv2 e o IGMPv3 não são apenas um protocolo, mas também um protocolo IPv4 (especificamente, número de protocolo 2). Ele não é usado apenas como descrito nesses RFCs para relatar associação de grupo multicast, mas também por outros protocolos multicast IPv4, como DVMRP, PIM versão 1, mtrace e mrinfo. É importante lembrar disso ao tentar filtrar o IGMP (via ACLs Cisco IOS®, por exemplo). No IPv6, o MLD não é um protocolo IPv6; em vez disso, o ICMPv6 é usado para transportar pacotes MLD. O PIM versão 2 é do mesmo tipo de protocolo em IPv4 e IPv6 (número de protocolo 103).

Pacotes de Controle PIM

Nesta seção, os pacotes de controle PIM multicast e unicast são discutidos. O RP automático e o Roteador de bootstrap (BSR), que são formas de selecionar pontos de reunião e controlar atribuições de Grupo a RP em redes PIM-SM, são discutidos.

Pacotes de Controle PIM Multicast

Os pacotes de controle PIM multicast incluem:

- PIM Hello - o pacote PIM Hello é um pacote multicast IP de escopo local de link enviado a um roteador conectado à mesma rede para estabelecer vizinhos PIM.
- PIM Join/Prune - PIM Join/Prunes são pacotes multicast IP de escopo local de link enviados para criar/remover o estado multicast e são enviados somente para vizinhos PIM. Eles são multicast dentro da LAN para facilitar asserção, supressão de relatório e outros detalhes do protocolo PIM, mas são sempre direcionados a um vizinho específico.
- PIM DF-Select - O PIM Designated Forwarder é o roteador PIM Bi-Dir responsável por (*,G)

JOINS enviados ao RP em nome dos receptores anexados ou vizinhos PIM downstream. Para os casos em que um roteador PIM detecta outro roteador que envia JOINS (*,G) no mesmo segmento para o mesmo grupo G, há uma eleição para determinar o roteador com o melhor caminho para o RP.

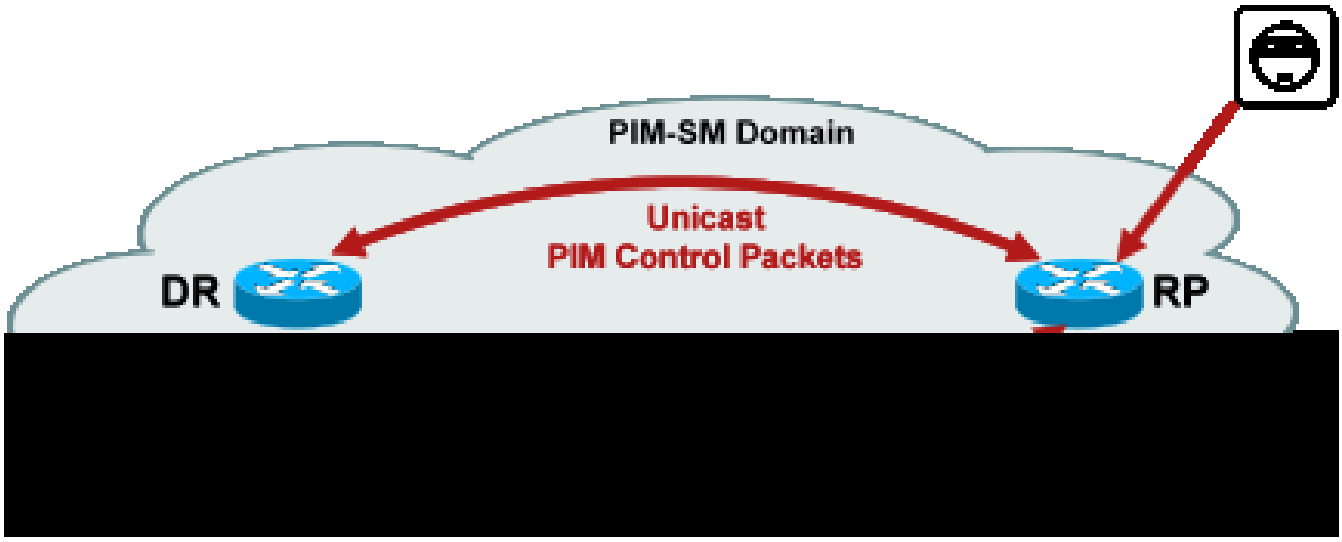
- PIM Assert - PIM Asserts são pacotes multicast IP de link local enviados quando um roteador PIM conectado a um segmento de rede que encaminha ativamente pacotes para um determinado (S,G) de uma determinada interface começa a RECEBER pacotes para o mesmo (S,G) na mesma interface na qual são encaminhados. Esse evento indica a presença de outro roteador que pensa ser o Encaminhador único (SF) para isso (S,G). O mecanismo Assert elege um SF exclusivo para isso (S,G). O roteador PIM SF é escolhido para encaminhar pacotes para um fluxo específico (S,G). O PIM permite que diferentes roteadores executem a função do SF em nome de diferentes (S,G)s, de preferência há apenas um SF por (S,G). Não confunda o SF com o Roteador designado. O roteador designado PIM é o roteador responsável por JOIN / PRUNES ou SOURCE REGISTERS que são enviados ao RP em uma rede PIM-SM.
- Bootstrap de PIM - As mensagens de bootstrap de PIM são enviadas em uma rede PIMv2 para facilitar a eleição dinâmica de um ponto de encontro para um grupo G específico.

Pacotes de Controle PIM Unicast

Os pacotes de controle PIM unicast são direcionados para ou do RP e incluem:

- Pacote de Registro de Origem - Os Pacotes de Registro de Origem PIM são enviados para registrar uma nova origem de multicast com um Ponto de Reunião. Assim que uma origem começa a enviar pacotes multicast, o roteador designado que está conectado à rede de origem envia um fluxo de registro unicast ao RP para indicar que há uma origem ativa presente para um grupo multicast pelo qual o RP é responsável.
  Os pacotes de registro de origem são enviados como um encapsulamento unicast do fluxo multicast original.
  As mensagens de registro PIM são comutadas em nível de processo e enviadas apenas até que o RP envie uma mensagem de interrupção de registro. O impacto no desempenho desses pacotes é proporcional à taxa de origem (por fluxo (S,G)).
- Register Stop Packet - Os pacotes de interrupção de registro do PIM são enviados do ponto de encontro para o PIM DR que enviou a mensagem de registro. As mensagens Register Stop são enviadas assim que o RP começa a receber pacotes multicast nativamente da origem.
- Pacote de anúncio de ponto de candidato-rendezvous do BSR - Pacotes de anúncio de C-RP do PIM BSR são enviados ao BSR para anunciar um RP candidato uma vez que o BSR é eleito.

Figura 1: Pacotes unicast PIM



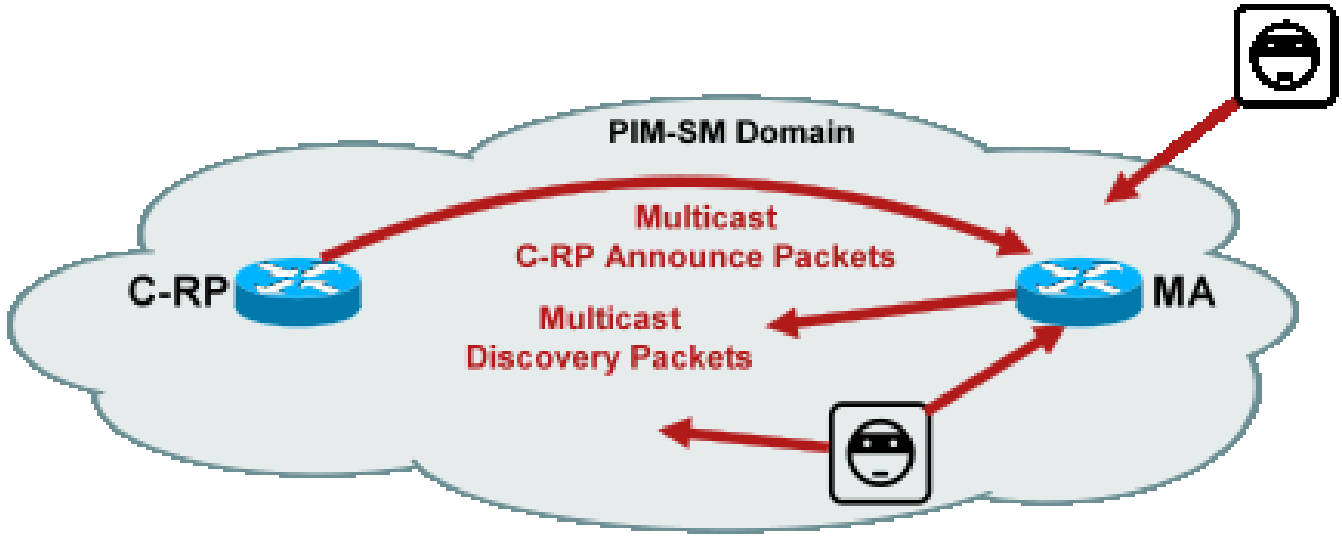
Os ataques que exploram esses pacotes podem se originar de qualquer lugar, pois esses pacotes são unicast.

Pacotes RP automático

O RP automático é um protocolo desenvolvido pela Cisco que tem a mesma finalidade que o PIMv2 BSR. O RP automático foi desenvolvido antes do BSR e suporta apenas IPv4. O BSR suporta IPv4 e IPv6. O agente de mapeamento no RP automático tem a mesma função que o roteador de bootstrap no BSR. No BSR, as mensagens do C-RP são unicast para o roteador de bootstrap. No RP automático, as mensagens são enviadas via multicast para o Agente de Mapeamento, o que permite filtros mais fáceis no limite, conforme descrito mais adiante. O RP automático é descrito em detalhes neste link:http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

No Cisco IOS, os pacotes AutoRP/BSR são sempre encaminhados e atualmente não são desativados. Isso pode apresentar uma exposição de segurança específica no caso do RP automático.

Figura 2: Pacotes AutoRP



Observação: embora o RP automático seja usado como um mecanismo para anúncio e descoberta de RP PIM-SM, ele não usa pacotes PIM (protocolo IP 103); em vez disso, ele usa pacotes de porta 496 do Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol) com endereços multicast.

Há dois tipos de pacotes usados pelo RP automático:

- Pacotes C-RP-Announce: esses pacotes são enviados por multicast a todos os agentes de mapeamento e usam um endereço "bem conhecido" reservado IANA (Internet Assigned Numbers Authority) (224.0.1.39). Eles são enviados por um C-RP para anunciar o endereço RP e o intervalo de grupos para os quais o RP pode atuar como o RP.
- Pacotes de descoberta C-RP: esses pacotes são multicast para todos os roteadores PIM e usam um endereço "bem conhecido" reservado IANA (224.0.1.40). Eles são enviados pelo Agente de mapeamento de RP automático para anunciar o C-RP específico que é eleito como o RP para um intervalo de grupo específico.

Cada um desses tipos de pacotes deve ser inundado pela rede.

No Cisco IOS, 224.0.1.39 e 224.0.1.40 são encaminhados no modo denso de PIM para evitar um problema de nenhum conhecimento anterior do RP para um grupo quando esse grupo é usado para distribuir informações de RP. Este é o único uso recomendado do Modo Denso de PIM.

No Cisco IOS XR, as mensagens de RP automático são mensagens de Encaminhamento de Caminho Reverso (RPF - Reverse Path Forwarding) inundadas salto por salto de vizinho para vizinho. Portanto, não há necessidade de criar um estado PIM DM mroute para suportar AutoRP no Cisco IOS XR. Na verdade, o Cisco IOS XR não suporta PIM-DM.

Pacotes MSDP (Multicast Service Discovery Protocol)

O MSDP é o protocolo IPv4 que permite que uma origem em um domínio seja anunciada a um receptor em outro domínio por meio de seus respectivos pontos de encontro. O MSDP é especificado no RFC 3618.

Para compartilhar informações sobre origens ativas entre domínios PIM, o MSDP é usado. Se uma origem se tornar ativa em um domínio, o MSDP garantirá que todos os domínios de peer aprendam sobre essa nova origem de forma oportuna, o que permitirá que os receptores em outros domínios rapidamente entrem em contato com essa nova origem se ela tiver sido enviada para um grupo no qual os receptores tenham interesse. O MSDP é necessário para comunicações multicast ASM / PIM-SM e é executado em uma conexão TCP (Transport Control Protocol) unicast configurada entre pontos de reunião nos respectivos domínios.

Ameaças em um ambiente multicast

Zonas de confiança e limites de confiança

Esta seção do documento é organizada por entidades funcionais na rede. O modelo de ameaça discutido é modelado em torno dessas entidades. Por exemplo, este documento explica como um roteador em uma rede multicast pode ser protegido (de um ponto de vista multicast), independentemente de onde o roteador é implantado. Da mesma forma, há considerações sobre como implantar medidas de segurança em toda a rede ou medidas em um roteador designado, ponto de encontro, etc.

As ameaças descritas aqui também seguem essa lógica e são organizadas por função lógica na rede.

Visão geral das ameaças

Em um nível abstrato, qualquer implantação de multicast pode estar sujeita a uma série de ameaças em vários aspectos de segurança. Os principais aspectos da segurança são confidencialidade, integridade e disponibilidade.

- Ameaças contra a confidencialidade: na maioria dos aplicativos, o tráfego multicast não é criptografado e, portanto, está aberto a qualquer pessoa para ouvir ou capturar qualquer elemento de linha ou de rede no caminho. Na seção sobre GET VPN, são discutidas formas de criptografar o tráfego multicast para evitar esses ataques.
- Ameaças contra a integridade do tráfego: sem segurança no nível do aplicativo ou segurança baseada em rede, como GET VPN, o tráfego multicast é vulnerável a modificações no trânsito. Isso é particularmente importante para o tráfego do plano de controle que usa multicast, como OSPF, PIM e muitos outros protocolos.
- Ameaças contra a integridade da rede: sem os mecanismos de segurança descritos neste documento, os remetentes, receptores ou elementos de rede comprometidos não autorizados podem acessar a rede multicast, enviar e receber tráfego sem autorização (roubo de serviço) ou sobrecarregar os recursos da rede.
- Ameaças contra a disponibilidade: há várias possibilidades de ataque de negação de serviço que podem tornar os recursos indisponíveis para usuários legítimos.

As próximas seções discutem as ameaças para cada função lógica na rede.

Ameaças básicas contra um roteador

Há uma série de ameaças fundamentais contra um roteador que são independentes de o roteador

suportar multicast e se o ataque envolve tráfego multicast ou protocolos.

Os ataques de negação de serviço (DoS) são os vetores de ataque genéricos mais importantes em uma rede. Em princípio, cada elemento de rede pode ser alvo de um ataque de DoS, que pode sobrecarregar o elemento com potencial perda ou degradação subsequente do serviço para usuários legítimos. É de suma importância seguir as recomendações básicas de segurança de rede que se aplicam ao unicast.

É importante observar que os ataques de multicast nem sempre são intencionais, mas frequentemente acidentais. Por exemplo, o worm Witty, observado pela primeira vez em março de 2004, é um exemplo de um worm que se espalha através de ataques aleatórios em endereços IP. Como consequência da completa aleatorização do espaço de endereços, os destinos IP multicast também foram afetados pelo worm. Em muitas organizações, vários roteadores do primeiro salto foram recolhidos porque o worm enviou pacotes para vários endereços de destino de multicast diferentes. Os roteadores, no entanto, não tinham escopo para essa carga de tráfego multicast com a criação de estado associada e experimentaram efetivamente o esgotamento de recursos. Isso ilustra a necessidade de proteger o tráfego multicast, mesmo que o multicast não seja usado em uma empresa.

As ameaças genéricas contra roteadores incluem:

- Inundações de pacotes de qualquer tipo; por exemplo, contra caminhos de hardware, como caminhos lentos (punt), e caminhos de software, como portas de plano de gerenciamento ou controle, que incluem Shell Seguro (SSH), Telnet, Border Gateway Protocol (BGP), OSPF, Network Time Protocol (NTP) e assim por diante
- Intrusões no roteador, com exploração subsequente de recursos no roteador; senhas Telnet ou SSH fracas e strings de comunidade SNMP fracas são um problema comum nas redes modernas.
- Problemas operacionais, como configurações incorretas ou ataques internos, podem colocar em risco a segurança de toda a rede e seu tráfego.

Quando o multicast é habilitado em um roteador, ele deve ser protegido além do unicast. O uso do multicast IP não altera o modelo de ameaça fundamental; no entanto, ele permite protocolos adicionais (PIM, IGMP, MLD, MSDP) que podem estar sujeitos a ataques, que precisam ser protegidos especificamente. Quando o tráfego unicast é usado nesses protocolos, o modelo de ameaça é idêntico a outros protocolos executados pelo roteador.

É importante observar que o tráfego multicast não pode ser usado da mesma forma que o tráfego unicast para atacar um roteador, pois o tráfego multicast é basicamente "orientado pelo receptor" e não pode ser direcionado a um destino remoto. Um destino de ataque precisa estar explicitamente "associado" ao fluxo de multicast. Na maioria dos casos (o RP automático é a

exceção principal), os roteadores escutam e recebem apenas o tráfego multicast "link local". O tráfego local de link nunca é encaminhado. Portanto, os ataques a um roteador com pacotes multicast só podem se originar de invasores diretamente conectados.

Ameaças da origem

Fontes multicast, sejam PCs ou servidores de vídeo, às vezes não estão sob o mesmo controle administrativo que a rede. Portanto, do ponto de vista do operador da rede, o remetente é tratado principalmente como não confiável. Dados os poderosos recursos dos PCs e servidores, e suas complexas configurações de segurança, que muitas vezes estão incompletas, os remetentes representam uma ameaça substancial contra qualquer rede, que inclui multicast. Essas ameaças incluem:

- Ataques da camada 2: há uma ampla gama de formas de ataque na camada 2 para realizar vários tipos de ataques. Eles se aplicam ao unicast e ao multicast. Como esses formulários de ataque não são específicos do multicast, eles não são discutidos com mais detalhes neste documento. Para obter mais informações, consulte o Cisco Press book "Segurança de switch LAN", ISBN-10: 1-58705-467-1.
- Ataques com tráfego multicast: como descrito anteriormente, é difícil conduzir ataques com tráfego multicast, já que o roteador do primeiro salto não encaminha tráfego multicast, a menos que haja um ouvinte para o grupo. No entanto, o primeiro salto pode ser atacado de várias maneiras com pacotes multicast:
    - Ataques de saturação de rede: um invasor pode inundar um segmento com pacotes multicast, sobre a utilização da largura de banda disponível, o que pode levar a uma condição de DoS.
    - Ataques de estado multicast: o roteador do primeiro salto é inundado com pacotes multicast, que podem criar muitos estados e uma condição de ataque DoS consequente.
    - Um remetente pode tentar se tornar o PIM DR, por meio de saudações PIM enviadas. Nesses casos, nenhum tráfego seria encaminhado de ou para a LAN.
    - Os pacotes de eleição de PIM DF para um BiDir-PIM DF podem ser falsificados. Nesses casos, nenhum tráfego seria encaminhado de ou para a LAN.
    - Um remetente pode falsificar mensagens de descoberta de RP de AutoRP ou de bootstrap de BSR. Isso efetivamente anunciaria um RP falso e desativaria ou interromperia um serviço PIM-SM/BiDir.
    - Um remetente poderia originar ataques unicast, como mensagens PIM source register/register-stop, ou enviar pacotes BSR anunciando e anunciando um BSR falso.
    - Um remetente pode enviar para qualquer grupo multicast válido, a menos que isso seja filtrado. Se um endereço de origem for falsificado e não for impedido na borda, o remetente poderá usar o endereço IP de origem de um remetente legítimo e substituir o conteúdo em partes da rede.
    - Ataques multicast contra protocolos de plano de controle: vários protocolos não associados ao multicast, como OSPF e Dynamic Host Configuration Protocol (DHCP), usam pacotes multicast, que podem ser usados para atacar esses protocolos

- Mascaramento: há várias formas de ataque nas quais um remetente pode fingir ser outro remetente. Os endereços IP de origem falsificados são uma dessas formas de ataque.
- Roubo de serviço: a menos que os remetentes sejam controlados, é possível usar o serviço multicast ilegitimamente do lado do remetente.

Observação: os hosts normalmente não enviam nem recebem pacotes PIM. O host que fizer isso provavelmente tentará um ataque.

Ameaças do lado do receptor

O receptor também é tipicamente uma plataforma com significativa potência de CPU e largura de banda, e permite um número de formas de ataque. Esses são basicamente idênticos às ameaças do lado do remetente. Os ataques de Camada 2 continuam sendo um importante vetor de ataque. Receptores falsos e roubo de serviço também são possíveis no lado do receptor, exceto que o vetor de ataque é tipicamente IGMP (ou ataques de camada 2, como mencionado).

Ameaças contra um ponto de encontro e BSR

Os PIM-SM RPs e PIM-BSRs são pontos críticos em uma rede multicast e, portanto, são alvos valiosos para um invasor. Quando nenhum dos dois é o roteador do primeiro salto, somente os formulários de ataque unicast, que incluem o unicast PIM, podem ser direcionados diretamente a esses elementos. As ameaças contra RPs e BSRs incluem:

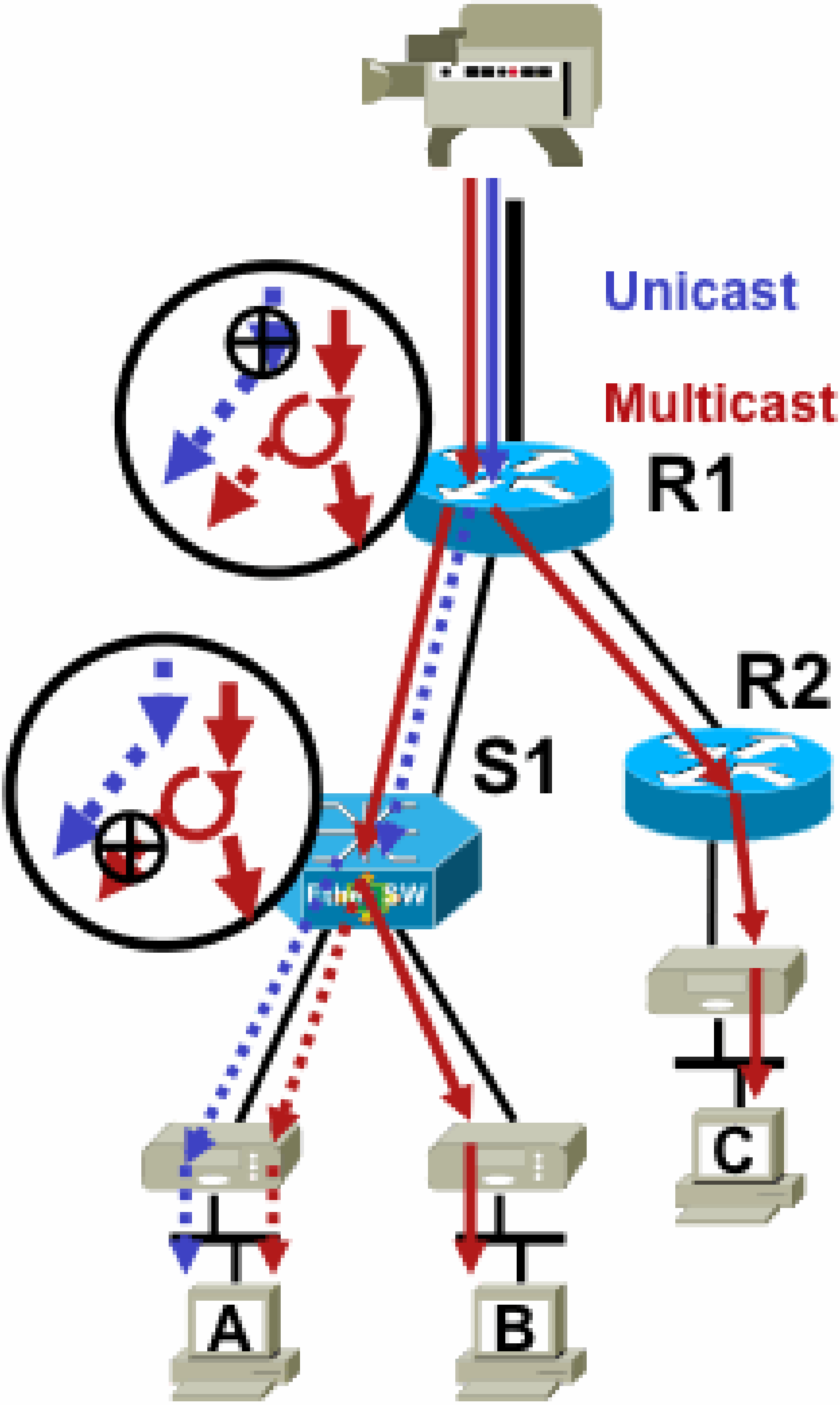
- Todos os formulários de ataque genéricos, conforme descrito na seção "Ameaças básicas contra um roteador".
- Ataques unicast PIM, potencialmente com endereços IP de origem falsificados, permitem ataques DoS, através de mensagens de registro PIM ou de interrupção de registro que são enviadas por um dispositivo mal-intencionado.

Segurança multicast e unicast (comparada)

Considerações/Filtros de estado

Considere a topologia na Figura 3, que mostra uma origem, três receptores (A, B, C), um switch (S1) e dois roteadores (R1 e R2). A linha azul representa um fluxo unicast e a linha vermelha representa um fluxo multicast. Todos os três receptores são membros do fluxo multicast.

Figura 3: Replicação em roteadores e switches


Unicast
Multicast
R1
R2
S1
A
B
C

- Para o fluxo multicast, no entanto, os administradores precisam ser mais específicos sobre onde instalar filtros: no filtro do lado do receptor após o último ponto de replicação antes do receptor; no filtro do lado da origem antes do primeiro ponto de replicação após a origem.

Ataques De Fontes Multicast

Esta seção se aplica aos modelos de serviço ASM e SSM, onde o tráfego é encaminhado com base no recebimento de junções explícitas do lado do receptor.

Para fluxos unicast, não há proteção implícita do receptor. Uma origem unicast pode enviar tráfego a um destino, mesmo que esse destino não tenha solicitado o tráfego. Portanto, mecanismos de defesa, como firewalls, são normalmente usados para proteger terminais. O multicast, por outro lado, tem alguma proteção implícita incorporada aos protocolos. O ideal é que o tráfego chegue apenas a um receptor que tenha entrado no fluxo em questão.

Com o ASM, as origens podem iniciar a inserção de tráfego ou ataques DoS através da transmissão de tráfego multicast para qualquer um dos grupos suportados por um RP ativo. Idealmente, esse tráfego não alcança um receptor, mas pode alcançar o roteador de primeiro salto no caminho no mínimo, assim como o RP, que permite ataques limitados. Se uma fonte mal-intencionada, no entanto, conhecer um grupo no qual um receptor de destino está interessado e se não houver filtros apropriados em vigor, ela poderá enviar tráfego para esse grupo. Esse tráfego é recebido desde que os receptores ouçam o grupo.

Com o SSM, os ataques de fontes indesejadas só são possíveis no roteador do primeiro salto, onde o tráfego para se nenhum receptor tiver ingressado nesse canal (S,G). Isso não leva a nenhum ataque de estado no roteador do primeiro salto porque ele descarta todo o tráfego SSM para o qual não existe um estado de união explícito dos receptores. Nesse modelo, não é suficiente que uma origem mal-intencionada saiba em qual grupo um destino está interessado, pois as "junções" são específicas da origem. Aqui, os endereços IP de origem que são falsificados mais possíveis ataques de roteamento seriam necessários para obter êxito.

Ataques de Estado

Mesmo sem os receptores presentes em uma rede, o PIM-SM cria o estado (S,G) e (*,G) no roteador do primeiro salto mais próximo da origem e também no ponto de encontro. Assim, existe a possibilidade de um ataque de estado na rede no roteador de primeiro salto de origem e no RP PIM-SM.

Se uma origem mal-intencionada começar a enviar tráfego para vários grupos, para cada um dos grupos detectados, os roteadores na rede criarão o estado na origem e no RP, desde que os grupos em questão sejam permitidos pela configuração do RP.

Portanto, o PIM-SM está sujeito a ataques de estado e de tráfego por fontes. O ataque pode ser agravado se a origem alterar seu endereço IP de origem aleatoriamente dentro do prefixo correto ou, em outras palavras, somente os bits de host do endereço serão falsificados.

Figura 4: Ataques ASM RP

Asm/
Bidir
ASM
/PIM-SM
Ouch
First
Hop
router
RP

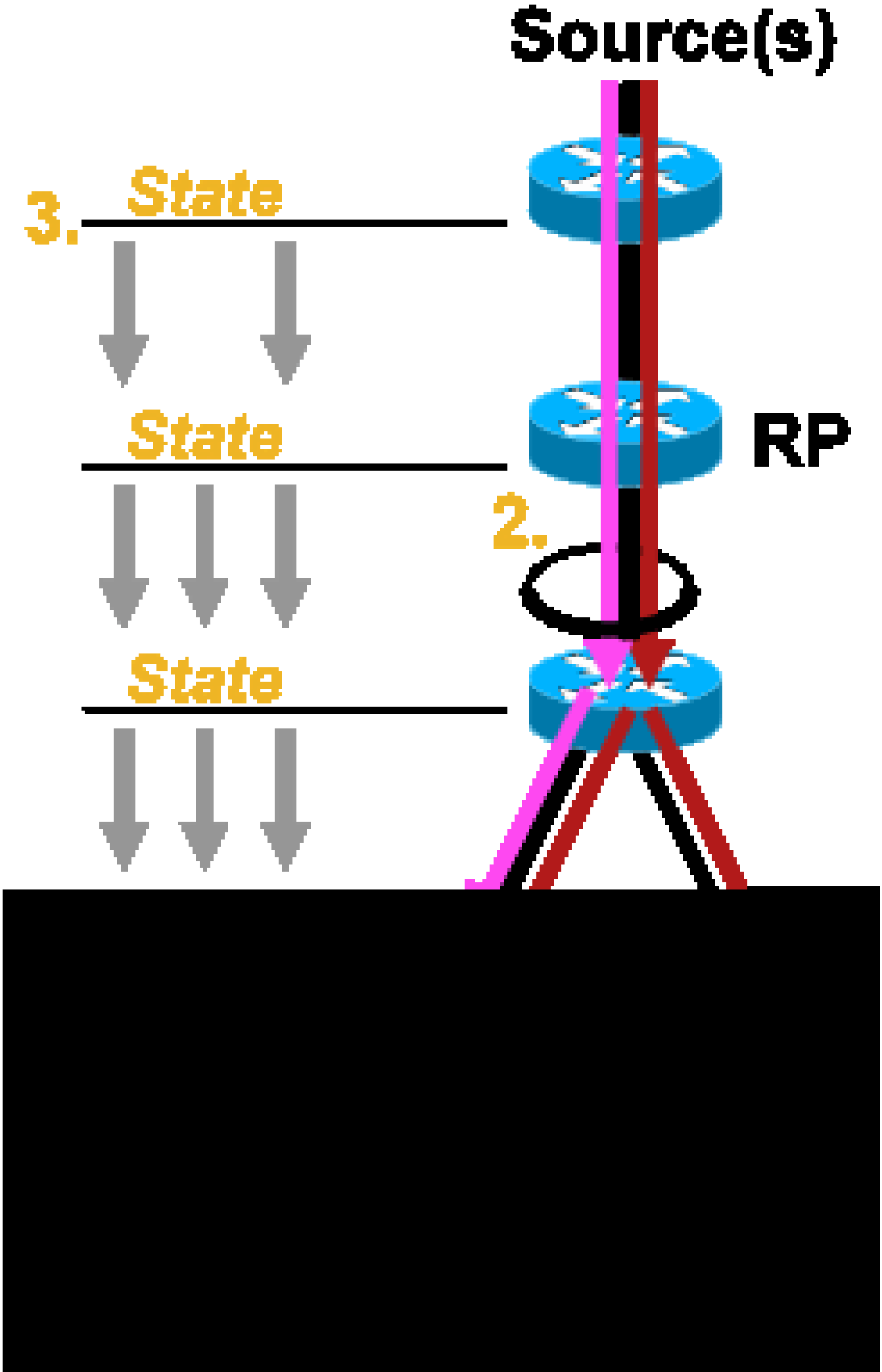
Assim como no PIM-SSM, os ataques de criação de estado PIM-BiDir a partir de fontes são impossíveis. O tráfego no PIM-BiDir é encaminhado no estado criado por junções de receptores, bem como no tráfego encaminhado de estado para o RP, de forma que ele possa alcançar receptores atrás do RP, já que as junções só vão para o RP. O tráfego de estado a encaminhar para o RP é chamado de estado (*,G/M) e é criado pela configuração do RP (estático, RP automático, BSR). Não muda na presença de fontes. Portanto, os invasores podem enviar tráfego multicast para um PIM-BiDir RP, mas, ao contrário do PIM-SM, um PIM-BiDir RP não é uma entidade "ativa" e, em vez disso, apenas encaminha ou descarta o tráfego para grupos PIM-BiDir.

Observação: em algumas plataformas Cisco IOS (*,G/M), o estado não é suportado. Nesses casos, as origens podem atacar o roteador por transmissão de tráfego multicast para vários grupos PIM-BiDir, o que causa a criação do estado (*,G). Por exemplo, o switch Catalyst 6500 suporta (*,G/M) estados.

Ataques iniciados pelo receptor

Os ataques podem se originar de receptores multicast. Qualquer receptor que envie relatórios de IGMP/MLD normalmente cria estado no roteador do primeiro salto. Não há mecanismo equivalente em unicast.

Fig 5: Encaminhamento de tráfego baseado em junção explícita no lado do receptor


Source(s)
3.
State
State
RP
2.
State

1. Um receptor multicast pode tentar ingressar em um fluxo para o qual não está autorizado e tentar receber conteúdo que não está autorizado a receber.
2. Um receptor multicast pode sobrecarregar potencialmente a largura de banda da rede disponível através do interesse em muitos grupos ou canais. Esse tipo de ataque torna-se um ataque de largura de banda compartilhada contra outros receptores potenciais de conteúdo.
3. Um receptor multicast pode tentar lançar um ataque contra roteadores ou switches. Um grande número de relatórios IGMP pode ser gerado, o que pode criar uma grande quantidade de estado de árvore multicast e sobrecarregar potencialmente a capacidade do roteador. Isso, por sua vez, pode resultar em um aumento nos tempos de convergência de multicast ou em um DoS no roteador.

Várias maneiras de mitigar esses tipos de ataques na próxima seção, Segurança em uma rede multicast.

Segurança em uma rede multicast

Segurança de elemento de rede

A segurança não é um recurso pontual, mas uma parte intrínseca de cada projeto de rede. Como tal, a segurança deve ser considerada em todos os pontos da rede. É de suma importância que todos os elementos da rede estejam protegidos adequadamente. Um cenário de ataque possível, aplicável a qualquer tecnologia, é um roteador subvertido por um invasor. Quando um invasor tem o controle de um roteador, o invasor pode executar vários cenários de ataque diferentes. Cada elemento de rede deve, portanto, ser adequadamente protegido contra qualquer forma de ataque básico, bem como contra ataques específicos de multicast.

Política de plano de controle (CoPP)

CoPP é a evolução das ACLs de roteador (rACLs) e está disponível na maioria das plataformas. O princípio é o mesmo: somente o tráfego destinado ao roteador é policiado por CoPP.

A política de serviço usa a mesma sintaxe de qualquer política de qualidade de serviço, com mapas de política e mapas de classe. Portanto, ele estende a funcionalidade de rACLs (permitir/negar) com limitadores de taxa para determinado tráfego em direção ao plano de controle.

Observação: certas plataformas, como os switches da série Catalyst 9000, têm o CoPP habilitado por padrão e a proteção não é substituída. Consulte o guia CoPP para obter informações adicionais.

Se você decidir ajustar, modificar ou criar rACLS ou CoPP em uma rede ativa, deve-se tomar cuidado. Como ambos os recursos têm a capacidade de filtrar todo o tráfego para o plano de controle, todos os protocolos de plano de controle e gerenciamento necessários devem ser explicitamente permitidos. A lista de protocolos necessários é grande e pode ser fácil ignorar protocolos menos óbvios, como o Sistema de Controle de Acesso do Controlador de Acesso do Terminal (TACACS). Todas as configurações rACL e CoPP não padrão devem sempre ser testadas em um ambiente de laboratório antes da implantação em redes de produção. Além disso, as implantações iniciais precisam começar apenas com uma política de "permissão". Isso permite a validação de qualquer ocorrência inesperada com contadores de ocorrências de ACL.

Em um ambiente multicast, os protocolos multicast necessários (PIM, MSDP, IGMP, etc) devem ser permitidos em rACL ou CoPP para que o multicast funcione corretamente. É importante lembrar que o primeiro pacote em um fluxo multicast da origem em um cenário PIM-SM é usado como um pacote de plano de controle, para ajudar a criar um estado multicast, no plano de controle do dispositivo. Portanto, é importante permitir grupos multicast relevantes em rACL ou CoPP. Como há várias exceções específicas da plataforma, é importante consultar a documentação relevante e testar qualquer configuração planejada antes da implantação.

Serviço de transporte de pacote local (LPTS)

No Cisco IOS XR, o Local Packet Transport Service (LPTS) serve como um vigilante do tráfego para o plano de controle do roteador, semelhante ao CoPP no Cisco IOS. Além disso, o tráfego de recepção, que inclui tráfego unicast e multicast, pode ser filtrado e ter taxa limitada.

Segurança específica de multicast

Em uma rede habilitada para multicast, cada elemento de rede precisa ser protegido com recursos de segurança específicos para multicast. Eles são descritos nesta seção, para proteção genérica do roteador. Os recursos que não são necessários em todos os roteadores, mas apenas em locais específicos na rede, e os recursos que exigem interação entre roteadores (como autenticação PIM) são discutidos na próxima seção.

Limites de Mroute

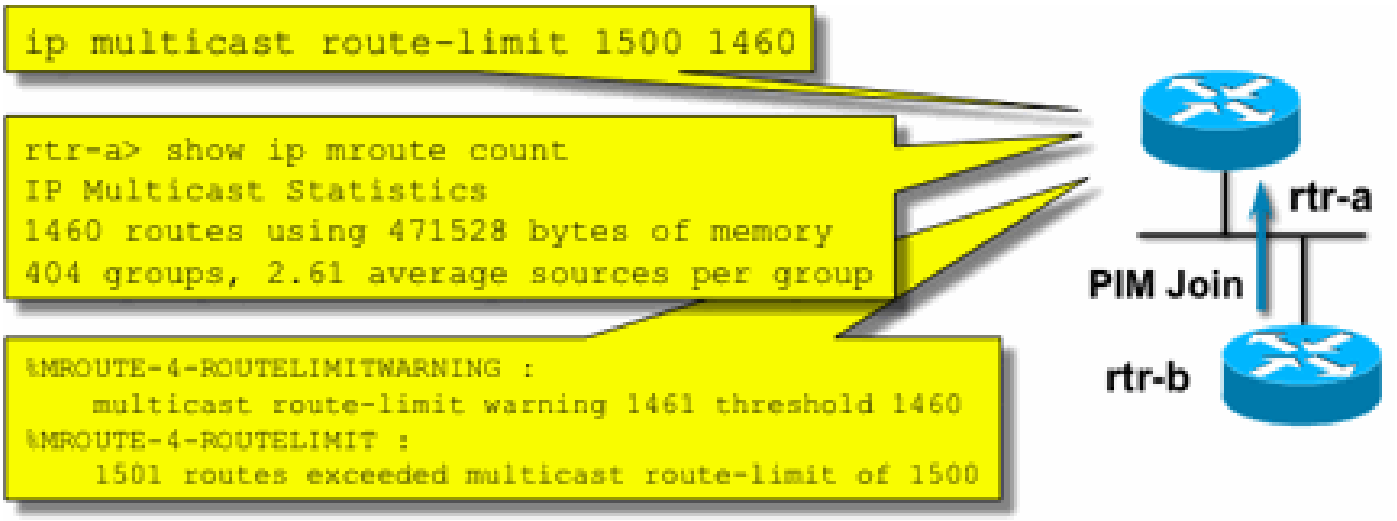
O comando mroute limit limita a quantidade de rotas multicast globalmente em um roteador e ajuda a evitar ataques de DoS.

<#root>

```
ip multicast route-limit

 <mroute-limit> <warning-threshold>
```

Fig 6: Limites De Mroute



Os limites de Mroute permitem a definição de um limite no número de mroutes permitidos na tabela de roteamento multicast. Se um limite de rota multicast estiver habilitado, nenhum estado multicast será criado além do limite configurado. Há também um limite de advertência. Quando o número de mroutes excede o limite de advertência, as mensagens de advertência syslog são disparadas. No limite mroute, todos os pacotes adicionais que acionariam o estado são descartados.

O comando ip multicast route-limit também está disponível por MVRF.

Desativar SAP Listen: no ip sap listen

O comando sap listen faz com que um roteador receba mensagens do Session Announcement Protocol/Session Description Protocol (SAP/SDP). O SAP/SDP é um protocolo legado que data dos dias do backbone multicast (MBONE). Essas mensagens indicam informações de diretório sobre o conteúdo multicast que estará disponível no futuro ou no presente. Isso pode ser uma origem de DoS contra recursos de CPU e memória do roteador e, portanto, esse recurso precisa ser desabilitado.

Controle o acesso às informações de mrinfo - o comando "ip multicast mrinfo-filter"

O comando mrinfo (disponível no Cisco IOS e também em algumas versões do Microsoft Windows e Linux) usa várias mensagens para consultar um roteador multicast para obter informações. O comando de configuração global ip multicast mrinfo-filter pode ser usado para limitar o acesso a essas informações a um subconjunto de fontes ou desabilitá-las completamente.

Este exemplo nega consultas originadas em 192.168.1.1, enquanto consultas são permitidas de qualquer outra origem:

```
ip multicast mrinfo-filter 51

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

Este exemplo nega mrinfo solicitações de qualquer origem:

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

 Observação: como esperado com qualquer ACL, um deny significa que o pacote está filtrado, enquanto um permit significa que o pacote está permitido.

Se o comando mrinfo for usado para fins de diagnóstico, é altamente recomendável configurar o comando ip multicast mrinfo-filter com uma ACL apropriada para permitir consultas somente de um subconjunto de endereços de origem. As informações fornecidas pelo comando mrinfo também podem ser recuperadas através do SNMP. Blocos completos de solicitações mrinfo (bloquear qualquer origem de consultas do dispositivo) são altamente recomendados.

Segurança de rede

Nesta seção, são discutidas várias maneiras de proteger pacotes de controle multicast e unicast PIM, bem como o RP automático e o BSR.

Desativar grupos multicast

Os comandos ip multicast group-range/ipv6 multicast group range podem ser usados para desabilitar todas as operações para grupos negados pela ACL:

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

Se os pacotes aparecerem para qualquer um dos grupos negados pela ACL, eles serão descartados em todos os protocolos de controle, que incluem PIM, IGMP, MLD, MSDP e também serão descartados no plano de dados. Portanto, nenhuma entrada de cache IGMP/MLD, PIM, estado de Base de Informações de Roteamento Multicast/Base de Informações de Encaminhamento Multicast (MRIB/MFIB) é criada para esses intervalos de grupos e todos os pacotes de dados são descartados imediatamente.

Esses comandos são inseridos na configuração global do dispositivo.

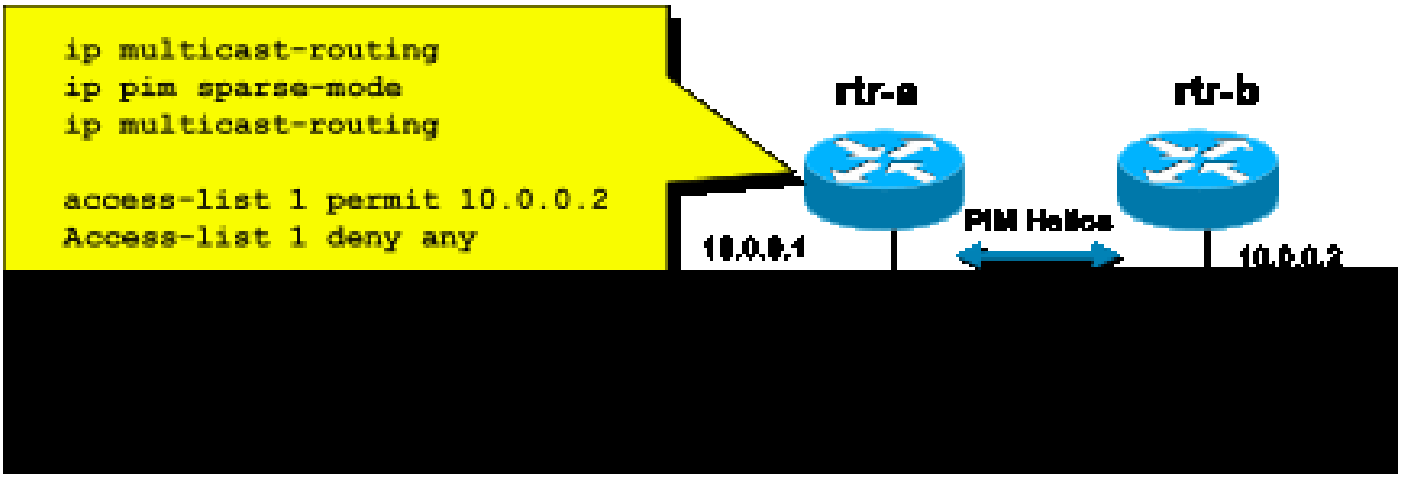
A recomendação é implantar esse comando em todos os roteadores da rede, quando e onde disponível, de modo que todo o tráfego multicast que se origina fora da rede seja controlado. Observe que esses comandos afetam o plano de dados e o plano de controle. Quando disponível, esse comando fornece uma cobertura mais ampla do que as ACLs padrão e é preferível.

Segurança PIM

Controle de Vizinho PIM

Um roteador PIM deve receber PIM Hellos para estabelecer a Vizinhança PIM. A Vizinhança PIM também é a base para a eleição do Designated Router (DR) e failover de DR, bem como mensagens PIM Join/Prune/Assert enviadas/recebidas.

Figura 7: Controle de vizinho PIM



Para inibir vizinhos indesejados, use o comando ip pim neighbor-filter ilustrado na Figura 7. Esse comando filtra de todos os pacotes PIM vizinhos não permitidos, o que inclui pacotes Hello, Join/Prune e pacotes BSR. Os hosts no segmento podem falsificar potencialmente o endereço IP de origem para fingir ser o vizinho PIM. Os mecanismos de segurança da camada 2 (ou seja, a proteção de origem IP) são necessários para impedir que os endereços de origem façam uma tentativa de spoof em um segmento ou usem uma VLAN ACL no switch de acesso para impedir que os pacotes PIM sejam enviados dos hosts. A palavra-chave "log-input" pode ser usada em ACLs para registrar pacotes que correspondam à ACE.

O pacote PIM Join/Prune é enviado a um vizinho PIM para adicionar ou remover esse vizinho de um caminho específico (S,G) ou (*,G). Os pacotes multicast PIM são pacotes multicast locais de link enviados com um Time-To-Live (TTL)=1. Todos esses pacotes são multicast para o endereço conhecido de todos os roteadores PIM: 224.0.0.13 . Isso significa que todos esses ataques devem se originar na mesma sub-rede que o roteador que é atacado. Os ataques podem incluir pacotes Hello, Join/Prune e Assert forjados.

Observação: um aumento artificial ou um ajuste do valor TTL em pacotes multicast PIM para

---

um valor maior que 1 não cria problemas. O endereço de todos os roteadores PIM é sempre recebido e tratado localmente em um roteador. Ele nunca é encaminhado diretamente por roteadores normais e legítimos.

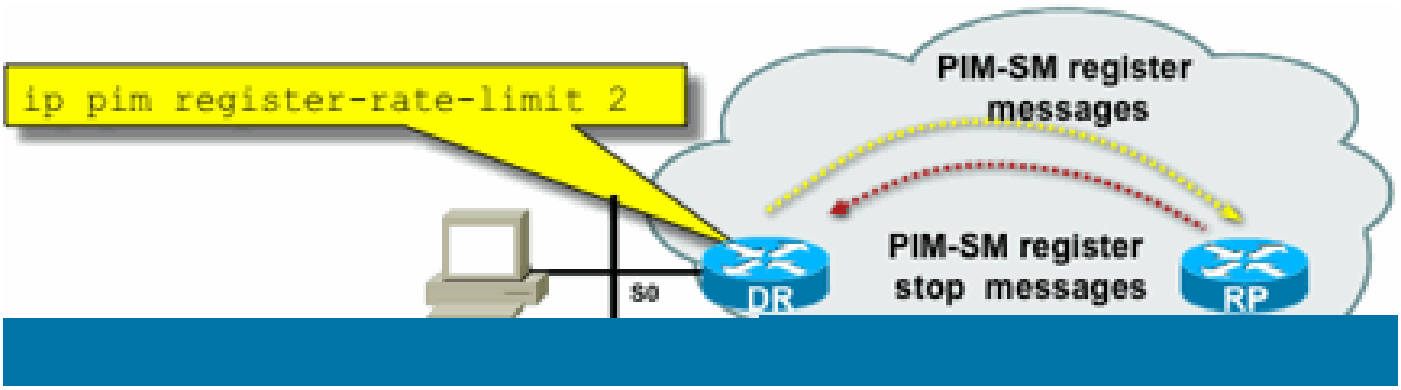
Para proteger o RP contra uma inundação potencial de mensagens de registro PIM-SM, o DR precisa limitar a taxa dessas mensagens. Use o comando ip pim register-rate-limit:

<#root>

ip pim register-rate-limit

<count>

Figura 8: Controle de túnel de registro PIM-SM



Pacotes PIM unicast podem ser usados para atacar o RP. Portanto, o RP pode ser protegido por ACLs de infraestrutura contra tais ataques. Lembre-se de que os remetentes e receptores multicast nunca precisam enviar pacotes PIM, de modo que o protocolo PIM (protocolo IP 103) pode geralmente ser filtrado na borda do assinante.

Controle de RP automático - Filtro de Anúncio RP

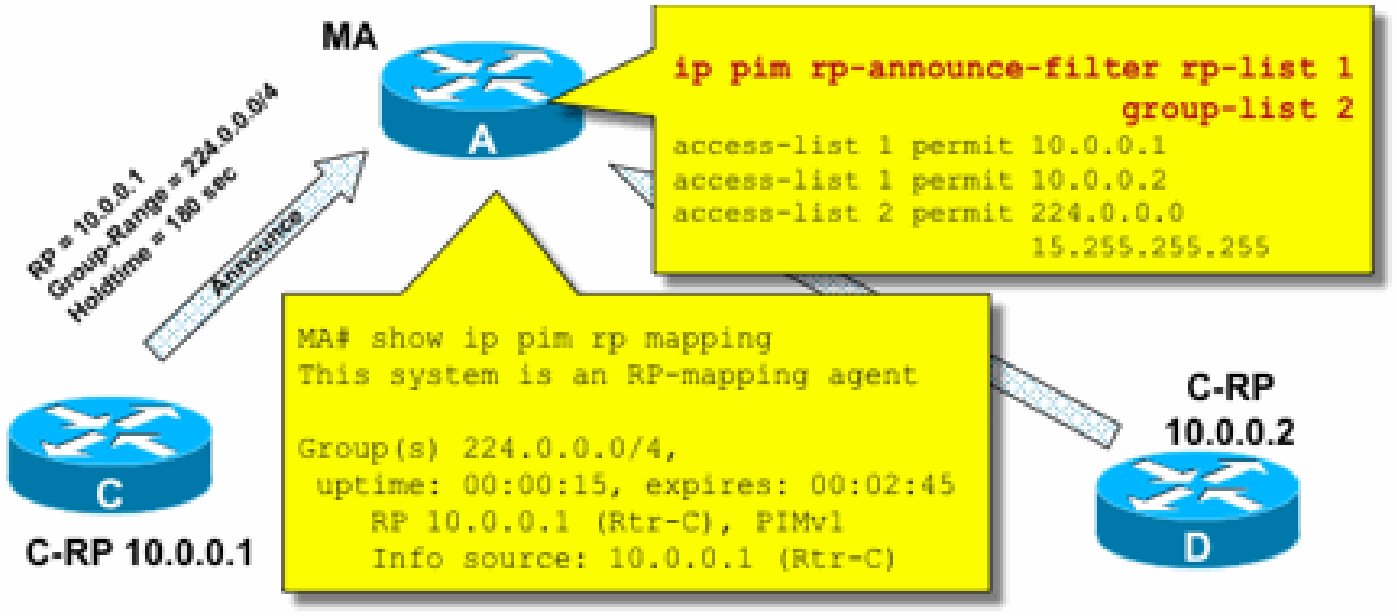
O comando ip pim rp-announce filter é uma medida de segurança adicional que pode ser configurada com AutoRP quando possível:

<#root>

ip pim rp-announce-filter

Isso pode ser configurado no Agente de Mapeamento para controlar quais roteadores são aceitos como RPs Candidatos para quais intervalos de grupo/modo de grupo.

Figura 9: RP automático - Filtro de anúncio RP



Controle de RP automático - Restringir mensagens de RP automático

Use o comando multicast boundary para restringir pacotes AutoRP, anúncio RP (224.0.1.39) ou descoberta RP (224.0.1.40) a um domínio PIM específico:

<#root>

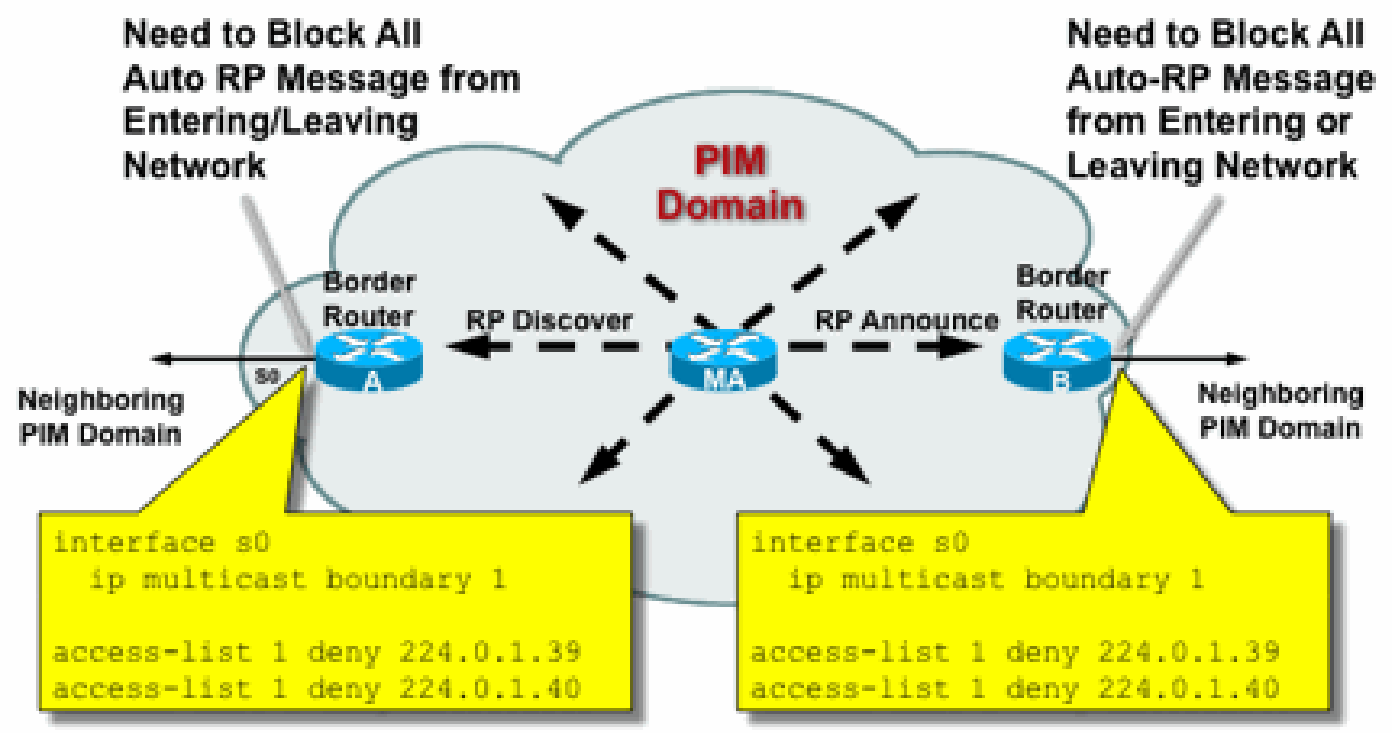
ip multicast boundary

access-list 1 deny 224.0.1.39

access-list 1 deny 224.0.1.40

224.0.1.39 (RP-announce) 224.0.1.40 (RP-discover)

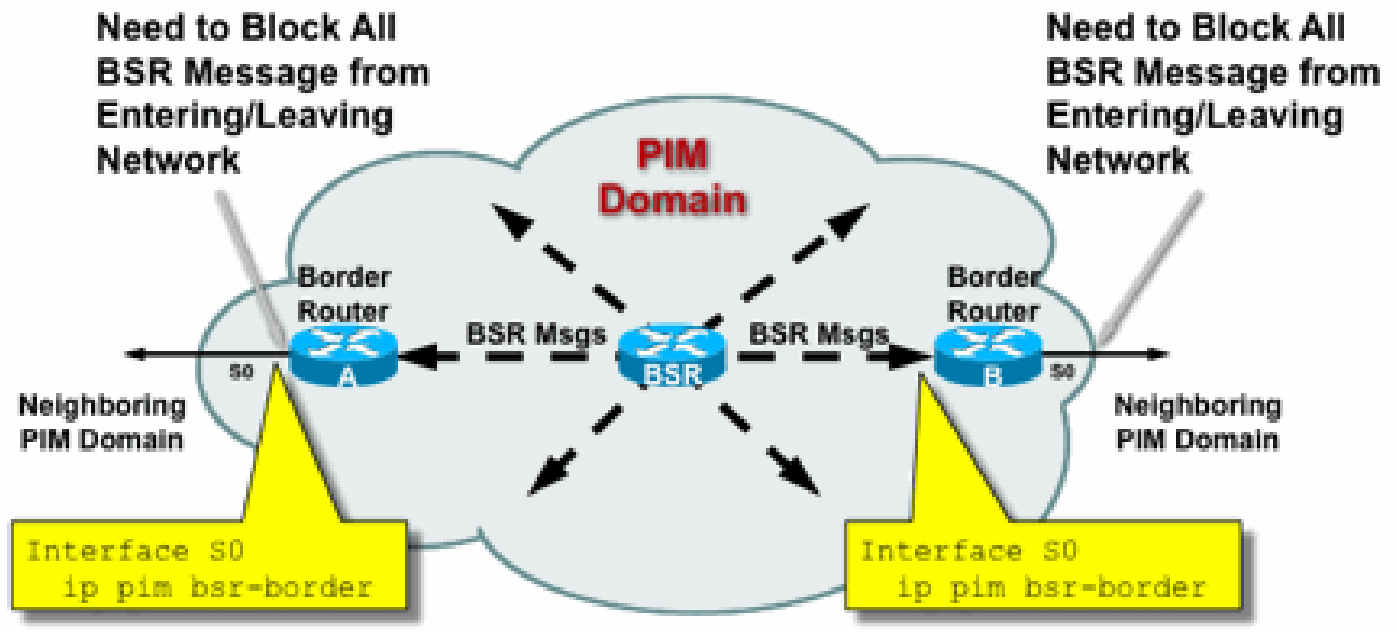
Figura 10: Comando Multicast Boundary



Controle de BSR - Restringir mensagens de BSR

Use o ip pim bsr-border para filtrar mensagens BSR na borda de um domínio PIM. Nenhuma ACL é necessária, já que as mensagens BSR são encaminhadas salto por salto com multicast de link local.

Figura 11: Borda do BSR



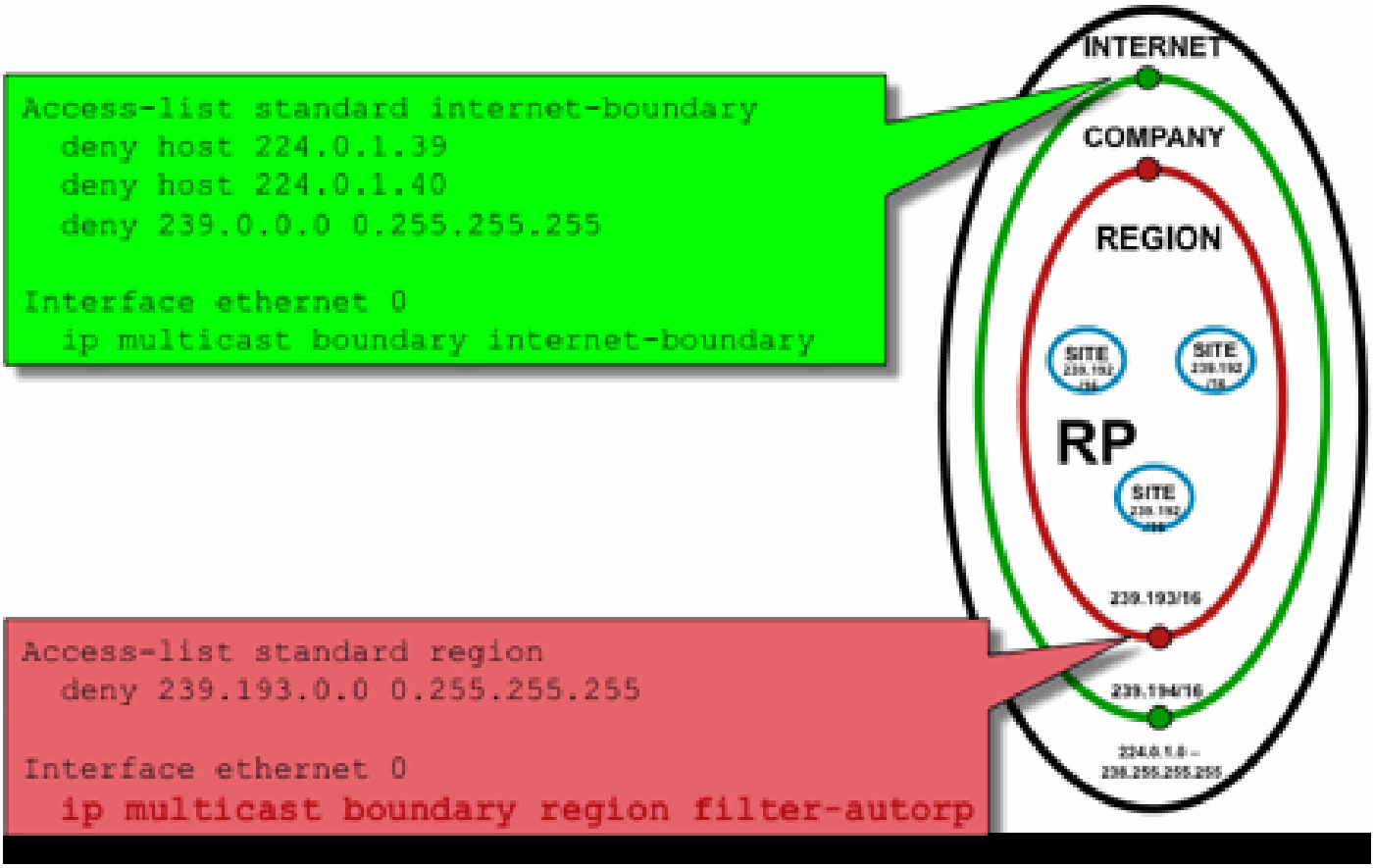
Filtros relacionados a RP / PIM-SM

Como parte desta seção final, são discutidos filtros contra pacotes de plano de controle PIM-SP e RP, bem como mensagens AutoRP, BSR e MSDP.

Filtros de RP automático

A Figura 12 mostra um exemplo de filtros de RP automático em conjunto com escopos de endereço. São mostradas duas formas diferentes de delimitar uma região. As duas ACLs são equivalentes de uma perspectiva de RP automático.

Fig 12: Filtros/escopos de RP automático



A ideia dos filtros de limite de interface para RP automático é garantir que os anúncios de RP automático atinjam apenas as regiões que eles suportam. Os escopos regional, da empresa e da Internet são definidos e, em cada caso, há anúncios RPs e AutoRP em cada escopo. Os administradores querem apenas que os RPs regionais sejam conhecidos pelos roteadores regionais, que os RPs da empresa sejam conhecidos pelos roteadores regionais e da empresa e que todos os RPs da Internet estejam disponíveis globalmente. São possíveis níveis adicionais de escopos.

Como mostrado na figura, há duas maneiras fundamentalmente diferentes de filtrar pacotes de RP automático: O limite da Internet chama explicitamente os grupos de controle de RP automático (224.0.1.39 e 224.0.1.40), o que resulta em filtros contra todos os pacotes de RP automático. Esse método pode ser usado na borda de um domínio administrativo, por onde nenhum pacote de RP automático é transmitido. O limite de Região usa a palavra-chave filter-auto-rp para causar um exame dos anúncios rp-to-group-range dentro de pacotes AutoRP. Quando um anúncio é explicitamente negado pela ACL, ele é removido do pacote AutoRP antes de o pacote ser encaminhado. No exemplo, isso permite que RPs em toda a empresa sejam conhecidos dentro das regiões, enquanto os RPs em toda a região são filtrados no limite da região para o resto da empresa.

Filtros entre domínios e MSDP

Neste exemplo, o ISP1 atua como um provedor de trânsito PIM-SM. Eles suportam apenas peering MSDP com vizinhos e aceitam apenas tráfego (S,G), mas nenhum tráfego (*,G) nos

roteadores de borda.

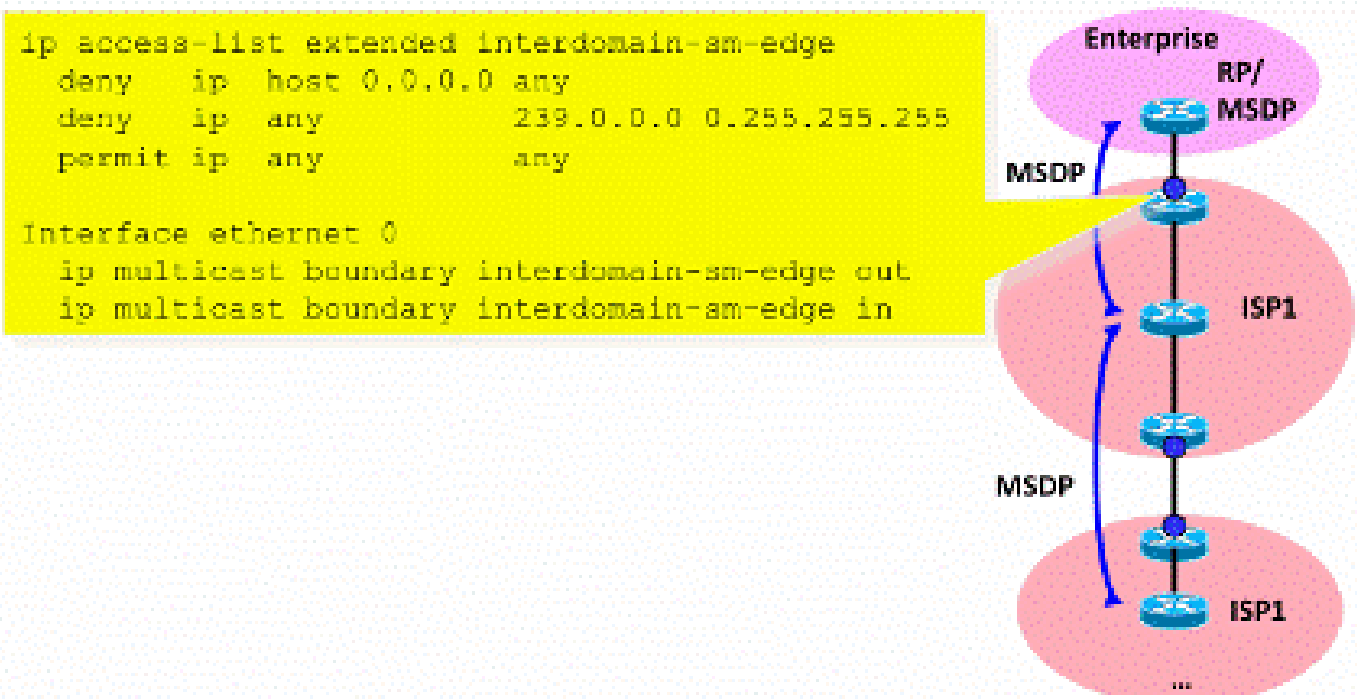
Em interdomínios (geralmente entre sistemas autônomos), há duas medidas básicas de segurança a serem tomadas:

1. Proteja o plano de dados por meio do comando multicast boundary. Isso garante que o tráfego multicast seja aceito apenas para grupos definidos (e origens potenciais).
2. Proteger o tráfego do plano de controle entre domínios (MSDP). Isso consiste em várias medidas de segurança separadas: controle de conteúdo MSDP, limitação de estado e autenticação de vizinhos.

A Figura 13 fornece um exemplo de configuração de um filtro de interface em um dos roteadores de borda do ISP1.

Para proteger o plano de dados no limite do domínio, iniba as junções (*,G) por filtros contra o "host 0.0.0.0" e endereços restritos administrativamente através do comando multicast boundary:

Figura 13: Filtro entre domínios (*,G)



Para proteger o plano de controle, fortaleça o MSDP por meio de três medidas básicas de segurança:

1) Filtros SA MSDP

É uma "prática recomendada" filtrar o conteúdo das mensagens MSDP por meio de filtros SA MSDP. A ideia principal desse filtro é evitar a propagação do estado de multicast para aplicativos e grupos que não sejam aplicativos em toda a Internet e não precisem ser encaminhados além do domínio de origem. Idealmente, do ponto de vista da segurança, os filtros permitem apenas grupos conhecidos (e potencialmente remetentes) e negam todos os remetentes e/ou grupos desconhecidos.

Geralmente, não é possível listar explicitamente todos os remetentes e/ou grupos permitidos. É recomendável usar o filtro de configuração padrão para domínios PIM-SM com um único RP para cada grupo (sem grupo de malha 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
         !
```

Recomenda-se filtrar o mais estritamente possível e em ambas as direções, entrada e saída.

Use para obter mais detalhes sobre as recomendações de filtro de SA do MSDP: https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) Limitação de estado MSDP

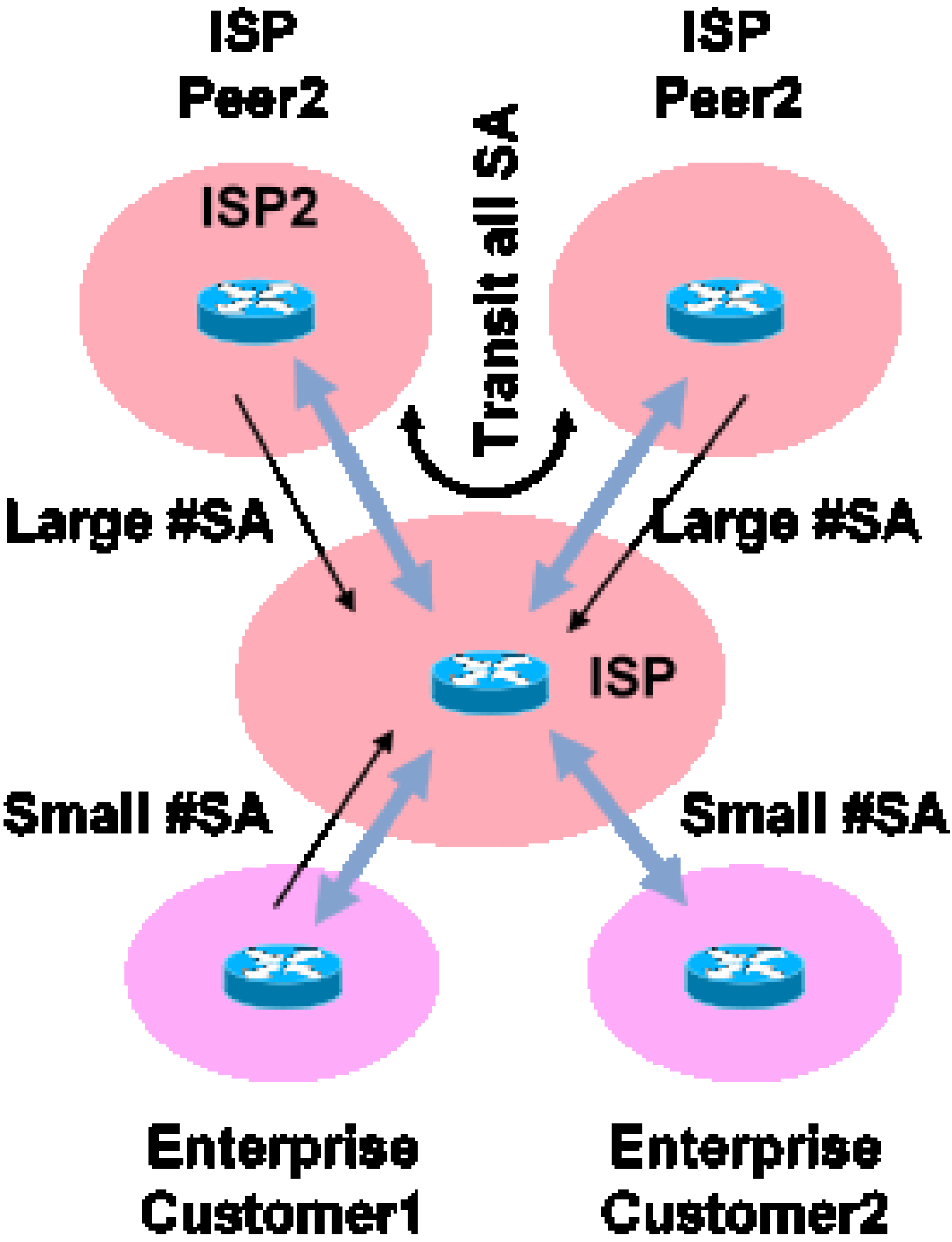
Quando o MSDP está habilitado entre vários sistemas autônomos (AS), é recomendável limitar a quantidade de estado que é criado no roteador devido às mensagens de "Origem Ativa" (SA) recebidas dos vizinhos. Você pode usar o comando ip msdp sa-limit:

<#root>

```
ip msdp sa-limit
```

```
 <peer> <limit>
```

Fig 14: Plano de controle MSDP



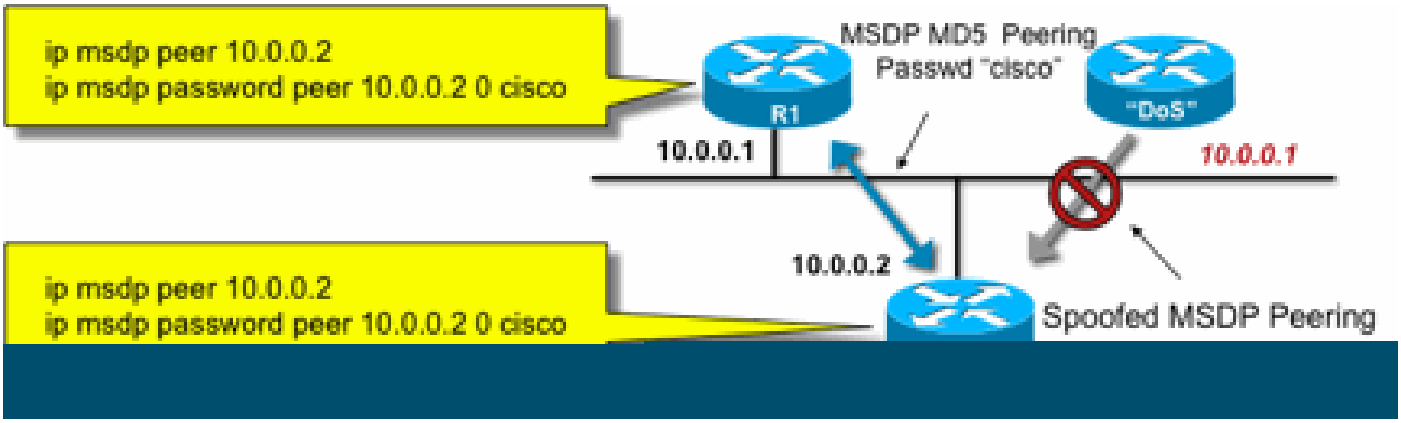
Com o comando ip msdp sa-limit você pode limitar o número de estados SA criados devido a mensagens SA aceitas de um peer MSDP. Algumas recomendações simples de regras fundamentais incluem:

- Limite pequeno do vizinho de stub
- Limite grande do vizinho de trânsito (por exemplo, #SAs máximo na Internet)
- ISP de trânsito - configure o máximo #SAs sua plataforma pode suportar

3) Autenticação de vizinhos MSDP MD5

Recomenda-se o uso da autenticação de senha do MD5 (Message-Digest Algorithm) em peers MSDP. Isso usa a opção de assinatura TCP MD5, equivalente ao uso descrito no RFC 6691 para proteger o BGP.

Fig 15: Autenticação de vizinhos MSDP MD5



Essas três recomendações de segurança do MSDP têm objetivos diferentes:

- A autenticação de vizinhos (com MD5) garante que somente pares MSDP confiáveis possam enviar mensagens.
- Os filtros de SA garantem que até mesmo um peer MSDP confiável possa apenas enviar anúncios de SA que estejam de acordo com a política de origem/grupo pré-acordada.
- O limite SA garante ainda que mesmo com anúncios legítimos (S,G) de pares legítimos, a memória disponível não pode ser esgotada.

Problemas de remetente/origem

Muitos problemas de segurança multicast que se originam no remetente podem ser atenuados com mecanismos de segurança unicast apropriados. Vários mecanismos de segurança unicast são práticas recomendadas aqui:

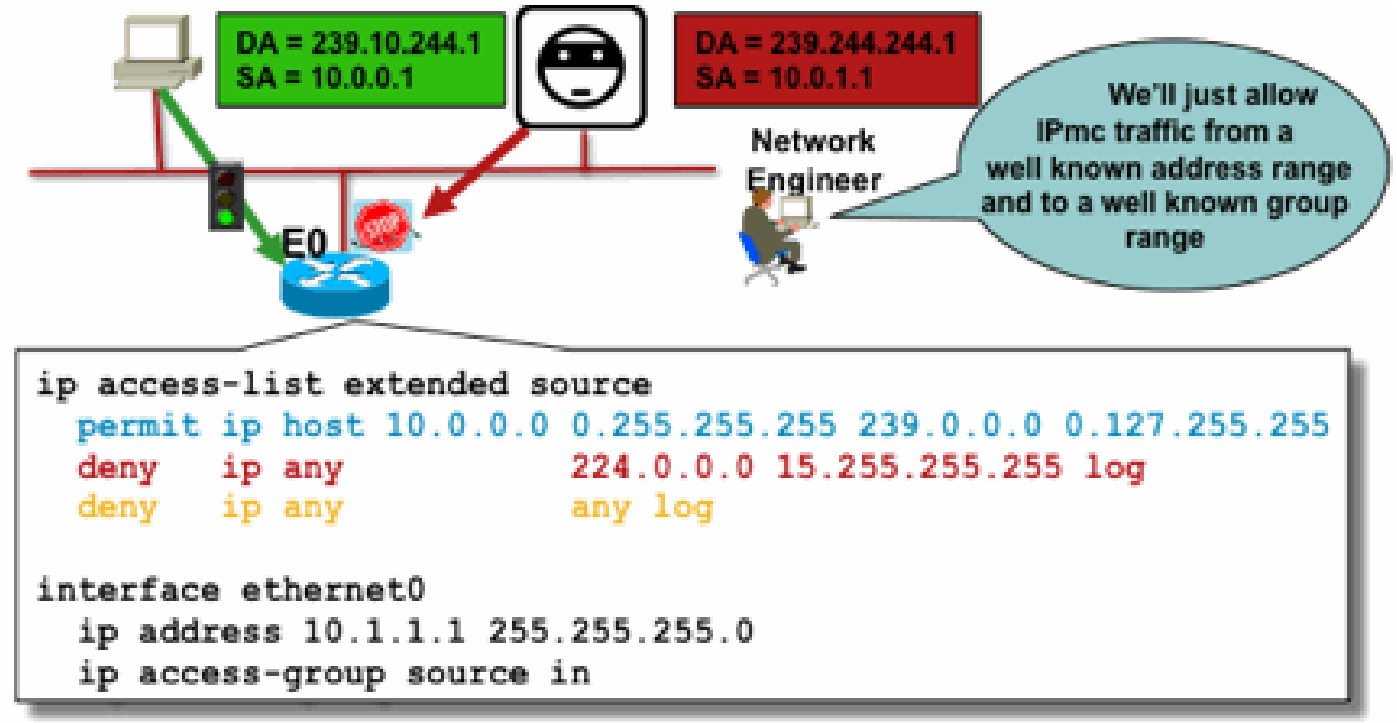
- Proteção de spoof de endereço de origem (Unicast Reverse Path Forwarding, uRPF ou ACL e IP source guard para a camada de acesso)
- ACLs de infraestrutura (deny ip any (to) <espaço de endereço central>)

Essas medidas podem ser usadas para bloquear ataques direcionados ao núcleo. Isso também resolveria, por exemplo, problemas como ataques que usam pacotes unicast PIM para o RP, que está "dentro" da rede e, portanto, seria protegido pela ACL de infraestrutura.

Controle de acesso com base em filtro de pacotes - Fontes de controle

No exemplo mostrado na figura 16, o filtro é configurado na interface LAN (E0) do roteador multicast do primeiro salto (roteador designado). O filtro é definido por uma lista de controle de acesso estendida chamada "origem". Essa ACL é aplicada à interface de origem do Roteador designado conectado à LAN de origem. Na verdade, devido à natureza do tráfego multicast, poderia haver a necessidade de um filtro similar configurado em todas as interfaces de LAN nas quais as origens poderiam se tornar ativas. Como não é possível em todos os casos saber exatamente onde ocorre a atividade de origem, é recomendável aplicar esses filtros em todos os pontos de ingresso na rede.

Figura 16: Fontes de controle



A finalidade desse filtro é impedir o tráfego de uma origem específica ou de um intervalo de endereços de origem para um grupo específico ou um intervalo de endereços de grupo. Esse filtro atua antes que o PIM crie qualquer mroutes e ajude a limitar o estado.

Esta é uma ACL de plano de dados padrão. Isso é implementado em ASICs em plataformas avançadas e não há nenhuma penalidade de desempenho. As ACLs do plano de dados são recomendadas e preferidas em relação ao plano de controle para fontes diretamente conectadas, pois minimizam qualquer impacto do plano de controle do tráfego indesejado. Também é muito eficaz limitar o destino (endereços de grupo multicast IP) para o qual os pacotes podem ser enviados. Como esse é um comando de roteador, ele não pode superar um endereço IP de origem que é falsificado (consulte a parte anterior desta seção). Portanto, recomenda-se fornecer mecanismos adicionais de camada 2 (L2) ou uma política consistente para todos os dispositivos que podem se conectar a uma rede local específica/rede local virtual (LAN/VLAN).

Observação: a palavra-chave "log" em uma ACL é muito útil para entender acertos em uma entrada de ACL específica; no entanto, isso consome recursos da CPU e precisa ser tratado com cuidado. Além disso, em plataformas baseadas em hardware, as mensagens de log da ACL são produzidas por uma CPU e, portanto, o impacto da CPU deve ser considerado.

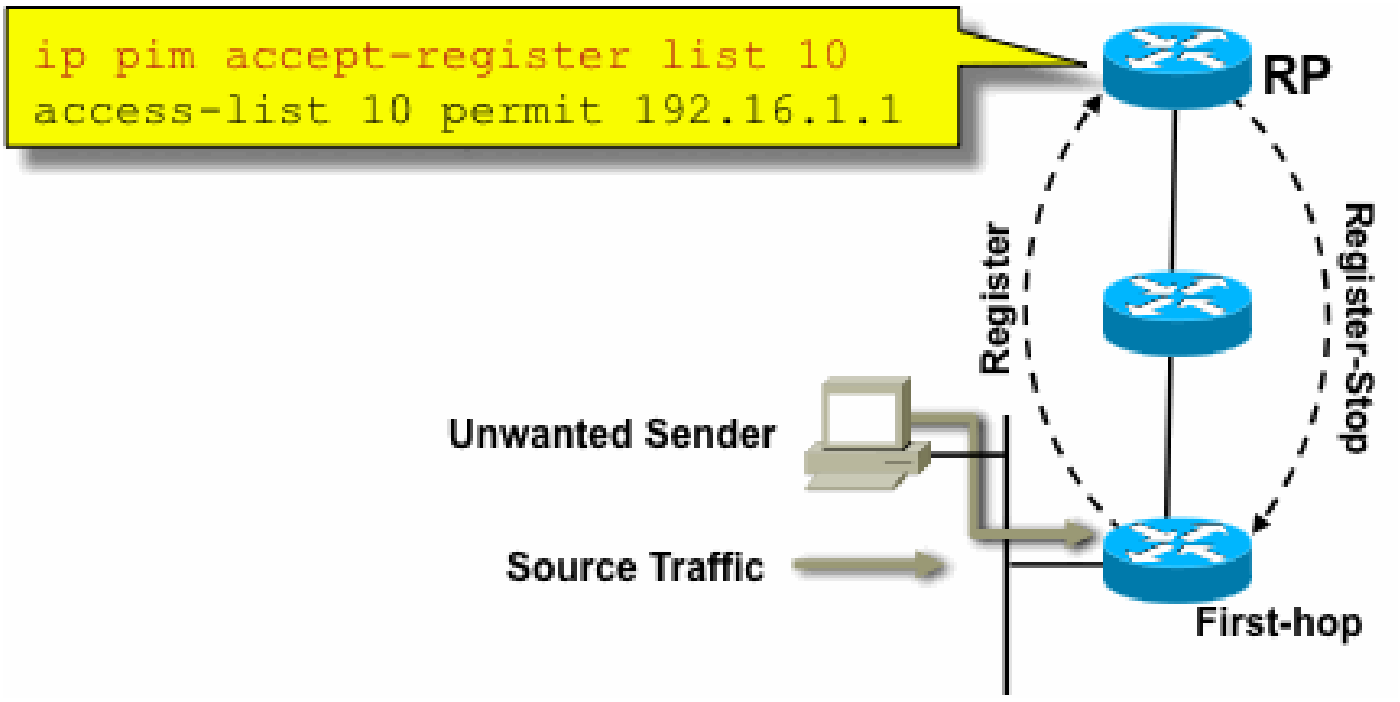
Controle de Origem PIM-SM

Uma das vantagens reais da arquitetura ASM / PIM-SM do ponto de vista da segurança é o fato de que o Ponto de Reunião fornece um único ponto de controle para todas as fontes na rede para qualquer intervalo de grupo. Isso pode ser aproveitado com um dispositivo chamado filtro de registro de aceitação. O comando para esse filtro é o seguinte:

<#root>

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

Figura 17: Controle de origem PIM-SM



Em uma rede PIM-SM, uma origem de tráfego indesejado pode ser controlada com esse comando. Quando o tráfego de origem atinge o roteador do primeiro salto, o roteador do primeiro salto (DR) cria o estado (S,G) e envia uma mensagem PIM Source Register ao RP. Se a origem não estiver listada na lista de filtros accept-register (configurada no RP), o RP rejeitará o Registro e enviará uma mensagem Register-Stop imediata ao DR.

No exemplo mostrado, uma ACL simples foi aplicada ao RP, que filtra somente no endereço de origem. Também é possível filtrar a origem E o grupo com o uso de uma ACL estendida no RP.

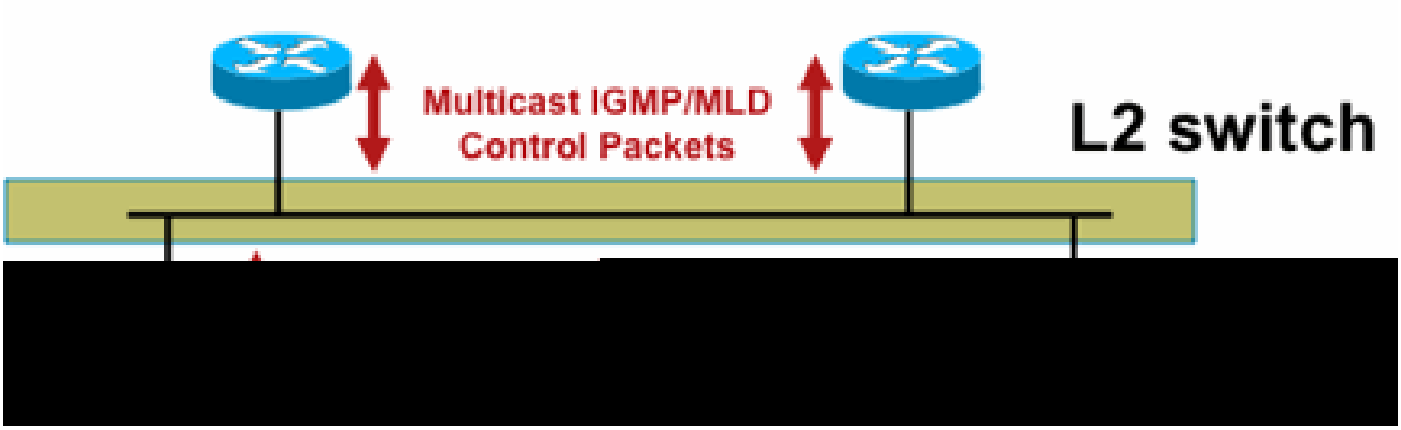
Há desvantagens com os filtros de origem, pois com o comando pim accept-register no RP, o estado PIM-SM (S,G) ainda é criado no roteador de primeiro salto da origem. Isso pode resultar em tráfego nos receptores locais para a origem e localizados entre a origem e o RP. Além disso, o comando pim accept-register funciona no plano de controle do RP. Isso pode ser usado para sobrecarregar o RP com mensagens de registro falsas e possivelmente causar uma condição de DoS.

É recomendável aplicar o comando pim accept-register no RP, além de outros métodos, como a aplicação de ACLs de plano de dados simples em todos os DRs, em todos os pontos de entrada na rede. Embora as ACLs de entrada no DR sejam suficientes em uma rede perfeitamente configurada e operada, é recomendável configurar o comando pim accept-register no RP como um mecanismo de segurança secundário em caso de configurações incorretas nos roteadores de borda. Mecanismos de segurança em camadas com o mesmo objetivo são chamados de "defesa aprofundada" e são um princípio de projeto comum em segurança.

Problemas do receptor - Controlar IGMP/MLD

A maioria dos problemas de receptor se enquadra no domínio das interações de protocolo do receptor IGMP/MLD.

Fig 18: Controlar IGMP



Quando os pacotes IGMP ou MLD forem filtrados, lembre-se destes pontos:

- IPv4: IGMP é um tipo de protocolo IPv4 (protocolo IPv4 2)
- IPv6: o MLD é transportado em pacotes de tipo de protocolo ICMPv6

O processo IGMP é ativado por padrão assim que o Multicast IP é ativado. Os pacotes IGMP também transportam esses protocolos e, portanto, todos esses protocolos são ativados sempre que o multicast é ativado:

- PIMv1 - PIMv1 foi a primeira versão do PIM e sempre está habilitado no Cisco IOS para fins de migração. Todas as implantações atuais usam PIMv2.
- Mrinfo - Mrinfo é um comando Unix que o Cisco IOS herdou para exibir vizinhos multicast. A Cisco recomenda o uso do SNMP em vez do comando mrinfo.
- DVMRP - DVMRP é um protocolo de vetor de distância de modo denso legado com

características de escalabilidade muito limitadas. O suporte do Cisco IOS para DVMRP foi desativado ou já foi preterido.
- Mtrace - O Mtrace é o equivalente multicast do "traceroute" unicast e é uma ferramenta útil

Para obter mais informações, consulte Internet Group Management Protocol (IGMP) Type Numbers da 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
```

Pacotes IGMP Unicast (para IGMP/UDLR) podem ser filtrados, pois são pacotes de ataque mais prováveis e não pacotes de protocolo IGMP válidos. Os pacotes de IGMP unicast são suportados pelo Cisco IOS no suporte de links unidirecionais e outras condições de exceção.

Pacotes de consulta IGMP/MLD forjados podem resultar em uma versão de IGMP mais baixa do que a esperada.

Em particular, os hosts idealmente nunca enviam consultas IGMP porque uma consulta enviada com uma versão IGMP mais baixa pode fazer com que todos os hosts que recebem essa consulta revertam para a versão mais baixa. Na presença de hosts IGMPv3 / SSM, isso pode "atacar" os fluxos SSM. No caso do IGMPv2, isso pode resultar em latências de saída mais longas.

Se uma LAN não redundante com um único consultante IGMP estiver presente, o roteador precisará descartar as consultas IGMP recebidas.

Se existir uma LAN passiva redundante/comum, será necessário um switch com capacidade de espionagem de IGMP. Há dois recursos específicos que podem ajudar nesse caso:

- Proteção do roteador
- comando Versão Mínima de IGMP

Proteção do roteador

Qualquer porta de switch pode se tornar uma porta de roteador multicast se o switch receber um pacote de controle de roteador multicast (IGMP general query, PIM Hello ou CGMP Hello) nessa porta. Quando uma porta de switch se torna uma porta de roteador multicast, todo o tráfego multicast é enviado para essa porta. Isso pode ser evitado com o "Router Guard". O recurso

Router Guard não exige que o rastreamento de IGMP esteja habilitado.

O recurso Router Guard permite que uma porta especificada seja designada como uma porta de host multicast. A porta não pode se tornar uma porta do roteador, mesmo que os pacotes de controle do roteador multicast sejam recebidos.

Esses tipos de pacotes serão descartados se forem recebidos em uma porta que tenha o Router Guard ativado:

- Mensagens de consulta IGMP
- Mensagens IPv4 PIMv2
- Mensagens IGMP PIM (PIMv1)
- Mensagens IGMP DVMRP
- Mensagens de Protocolo de Gerenciamento de Grupo (RGMP - Group Management Protocol) de porta de roteador
- Mensagens do Protocolo de Gerenciamento de Grupos (CGMP - Group Management Protocol) da Cisco

Quando esses pacotes são descartados, as estatísticas são atualizadas, indicando que os pacotes são descartados devido ao Router Guard.

Versão Mínima de IGMP

É possível configurar a versão mínima permitida dos hosts IGMP. Por exemplo, você pode não permitir todos os hosts IGMPv1 ou todos os hosts IGMPv1 e IGMPv2. Este filtro se aplica somente a relatórios de associação.

Se os hosts estiverem conectados a uma LAN "passiva" comum (por exemplo, um switch que não suporta Snooping IGMP ou que não está configurado para ele), também não haverá nada que um roteador possa fazer sobre essas consultas falsas, a não ser ignorar os relatórios de associação de "versão antiga" que são acionados e não se autorrecuperam.

Como as consultas de IGMP devem ser visíveis para todos os hosts, não é possível usar um mecanismo de autenticação de mensagem baseada em hash (HMAC) com uma chave pré-compartilhada, como IPSec de chave estática, para autenticar consultas de IGMP de "roteadores válidos". Se dois ou mais roteadores estiverem conectados a um segmento de LAN comum, será necessária uma eleição do consultante IGMP. Nesse caso, o único filtro que pode ser usado é um filtro ip access-group baseado no endereço IP de origem do outro roteador IGMP que envia consultas.

Pacotes IGMP multicast "normais" devem ser permitidos.

Esse filtro pode ser usado nas portas do receptor para permitir somente pacotes IGMP "bons" e para filtrar os "ruins" conhecidos:

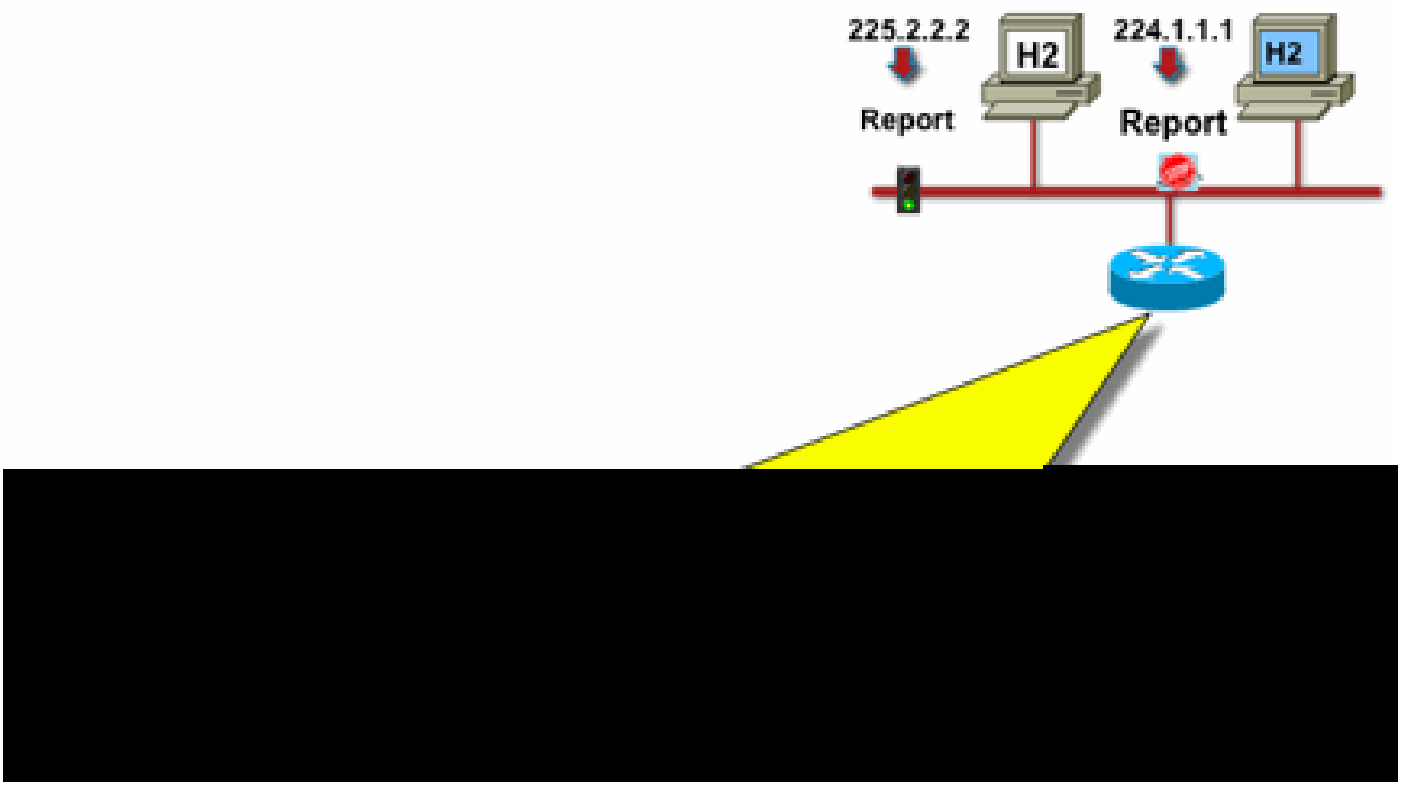
```
ip access-list extended igmp-control
   <snip>
   deny   igmp any any  pim        ! No PIMv1
```

```
   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
```

Observação: esse tipo de filtro IGMP pode ser usado em ACLs de recepção ou CoPP. Em ambos os aplicativos, ele precisa ser combinado com filtros para outro tráfego tratado, como protocolos de plano de roteamento e gerenciamento.

Fig 19: Controle De Acesso Do Lado Do Receptor Do Host



Para filtrar o tráfego para um receptor, não filtre o tráfego do plano de dados, mas o IGMP do protocolo de plano de controle. Como o IGMP é um pré-requisito necessário para receber tráfego multicast, nenhum filtro de plano de dados é necessário.

Em particular, você pode restringir quais receptores de fluxos multicast podem se unir (conectados à interface em que o comando está configurado). Nesse caso, use o comando ip igmp access-group / ipv6 mld access-group:

<#root>

ip igmp access-group / ipv6 mld access-group

Para grupos ASM, esse comando filtra apenas com base no endereço de destino. O endereço IP origem na ACL é ignorado. Para grupos SSM que usam IGMPv3 / MLDv2, ele filtra no IP de origem e de destino.

Este exemplo filtra um determinado grupo para todos os alto-falantes 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 exemplo filtra alto-falantes IGMP específicos (ou seja, receptores multicast específicos) para um determinado grupo:

```
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
```

 Observação: Lembre-se de que, para grupos ASM, a origem é ignorada.

Controle de Admissão

O controle de acesso fornece uma resposta binária, sim ou não para determinados fluxos, independentemente do estado da rede. O controle de admissão, por contraste, limita o número de recursos que um remetente/receptor pode usar, supondo que eles passaram pelos mecanismos de controle de acesso. Vários dispositivos estão disponíveis para ajudar com o controle de admissão em um ambiente multicast.

Limites IGMP globais e por interface

No roteador mais próximo dos receptores multicast interessados, existe a possibilidade de limitar o número de grupos IGMP unidos globalmente e por interface. Você pode utilizar os comandos ip igmp limit/ipv6 mld limit:

<#root>

```
ip igmp limit
```

```
 <n> [ except <ext-acl> ]
```

```
ipv6 mld limit
```

```
 <n> [ except <ext-acl> ]
```

Recomenda-se que esse limite seja sempre configurado por interface e também globalmente. Em cada caso, o limite se refere às contagens de entradas no cache IGMP.

Os próximos dois exemplos mostram como esse comando pode ser usado para ajudar a limitar o número de grupos na borda de uma rede de banda larga residencial.

Exemplo 1 - Restringir grupos recebidos somente aos anúncios SDR mais um canal recebido

O Diretório de Sessão (SDR) atua como um guia de canal para alguns receptores multicast. Consulte RFC 2327 para obter mais detalhes.

Um requisito comum é restringir os receptores a receberem o grupo SD mais um canal. Este exemplo de configuração pode ser usado:

```
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
```

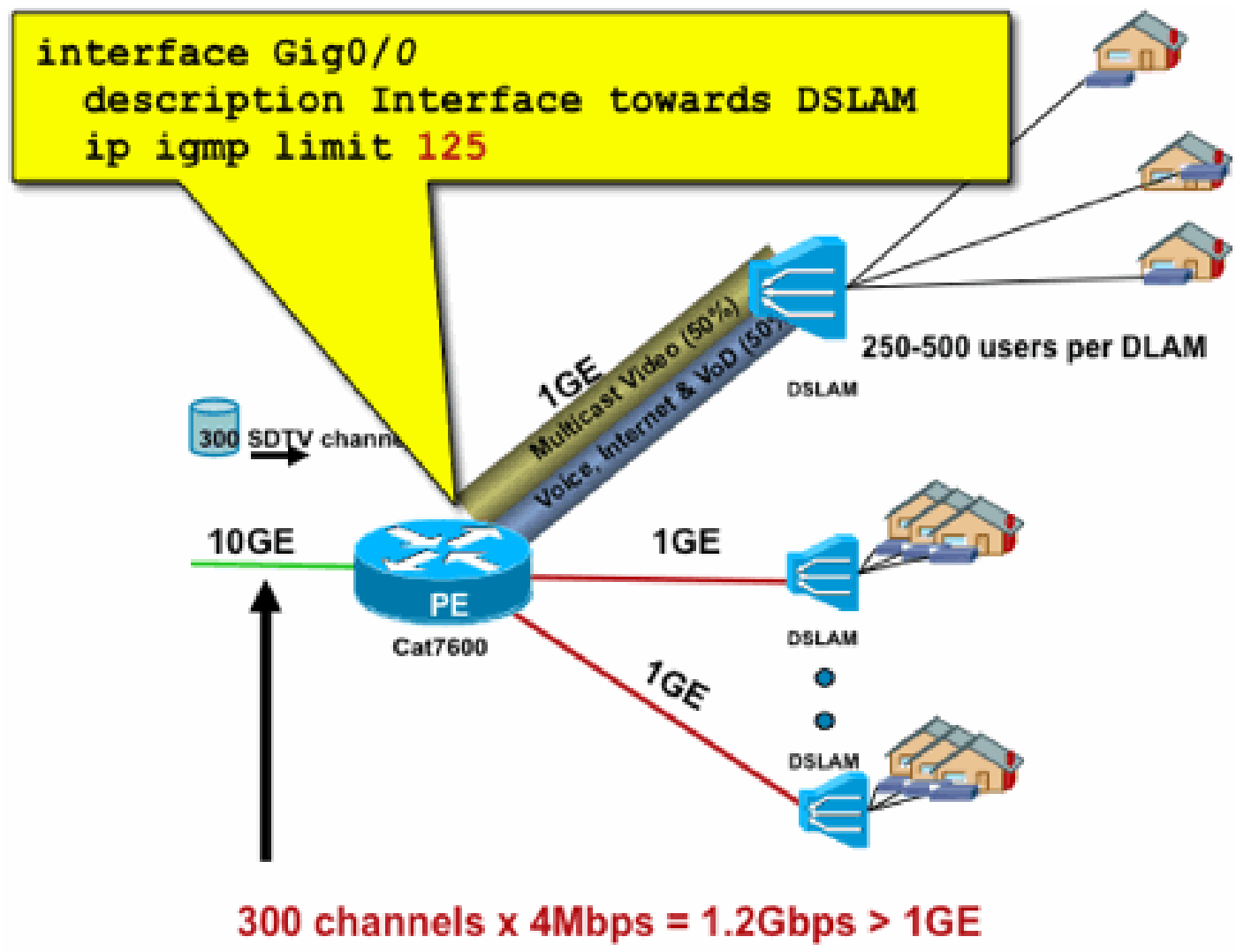
A lista de acesso neste exemplo especifica somente o guia de canal; o comando global ip igmp limit limita cada origem IGMP a um único canal (1), mas não inclui o guia de canal, que sempre pode ser recebido. O comando interface substitui o comando global e permite que dois (2) canais sejam recebidos, além do guia de canais, nessa interface.

Exemplo 2 - Controle de Admissão no Link Aggregation-DSLAM

Esse comando também pode ser usado para fornecer uma forma de controle de admissão de largura de banda. Por exemplo, se for necessário distribuir 300 canais SDTV, cada um com 4 Mbps, e houver um link de 1 Gbps para o DSLAM (Digital-Subscriber-Line-Access-Multiplexer, Multiplexador de acesso de linha de assinante digital), você poderá tomar uma decisão de política para limitar a largura de banda da TV a 500 Mbps e deixar o restante para a Internet e outros usos. Nesse caso, você pode limitar os estados de IGMP a 500 Mbps/4 Mbps = 125 estados de IGMP.

Esta configuração pode ser usada neste caso:

Fig 20 Uso de Limites IGMP por Interface; Controle de Admissão no Link Agg-DSLAM



Limites mroute por interface

A habilitação de limites de estado de mroute por interface é uma forma mais genérica de controle de admissão. Ele não apenas limita o IGMP e o estado PIM em uma interface de saída, mas também fornece uma forma de limites de estado em interfaces de entrada.

Use o comando ip multicast limit:

<#root>

ip multicast limit [rpf | out | connected]

<ext-acl> <max>

O estado pode ser limitado separadamente nas interfaces de entrada e saída. O estado de origem diretamente conectado também pode ser limitado com o uso da palavra-chave "connected". Exemplos ilustram o uso desse comando:

Exemplo 1 - Controle de admissão de saída no link Agg-DSLAM

Neste exemplo, há 300 canais de TV SD. Suponha que cada canal SD precise de 4 Mbps, com um total não superior a 500 Mbps. Por fim, suponha também que haja necessidade de suporte aos pacotes Basic, Extended e Premium. Exemplo de alocações de largura de banda:

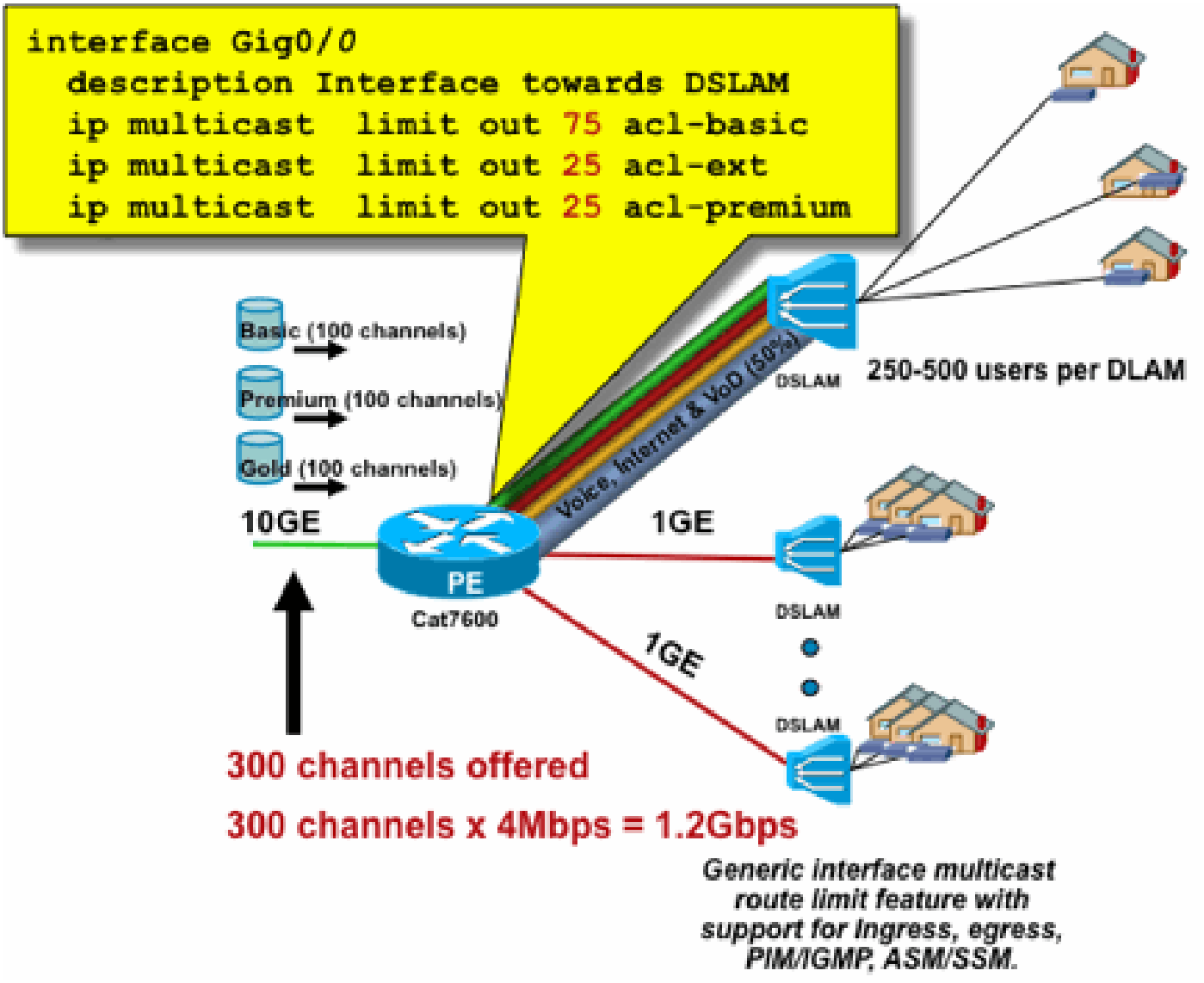
- Básico de 60%/300 Mbps
- 20%/100 Mbps estendido
- Premium de 20%/100 Mbps

Em seguida, use 4 Mbps por canal, limite o uplink DSLAM a:

- 75 estados básicos
- 25 estados estendidos
- 25 estados Premium

Configure o limite na interface de saída voltada para o DSLAM do PEAgg:

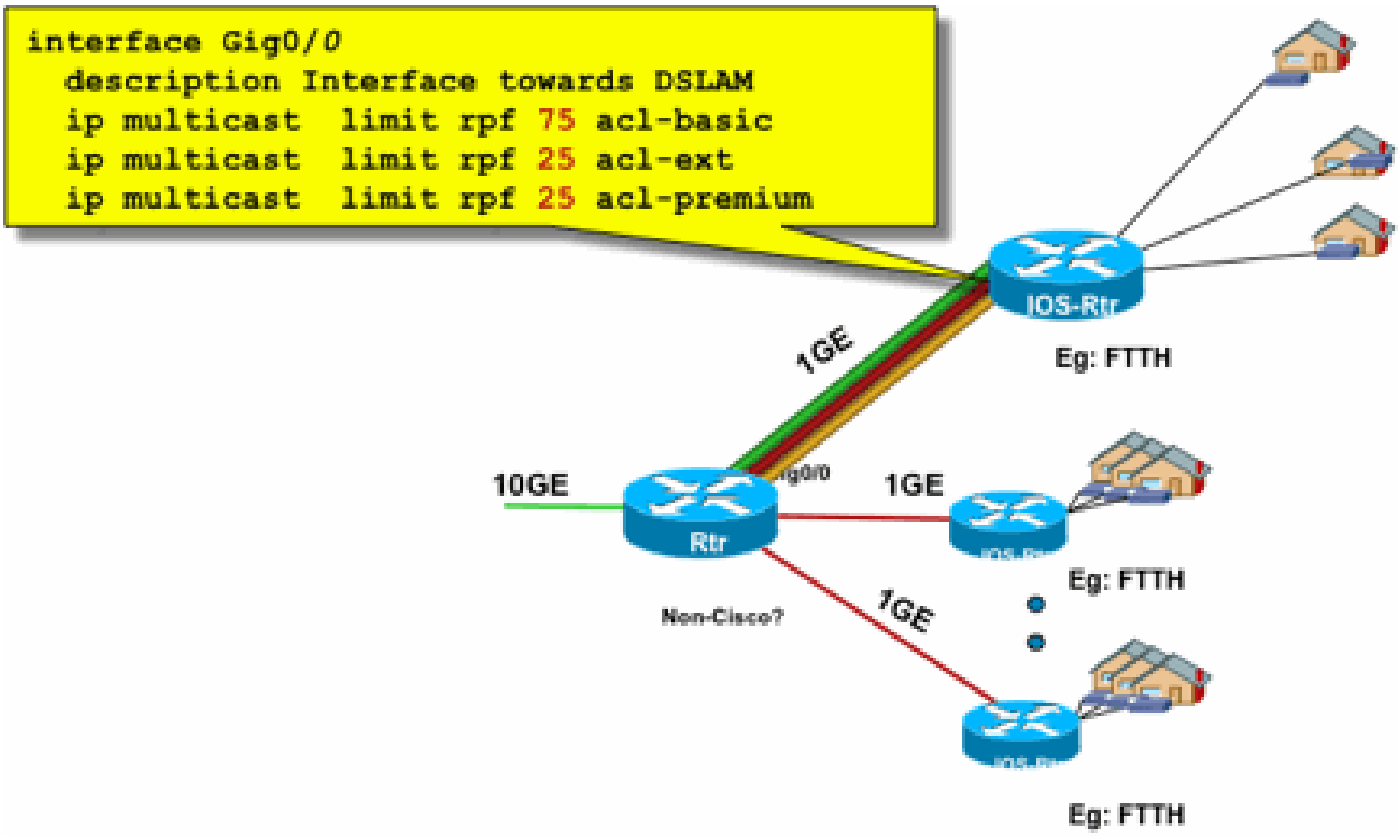
Fig 21: Uso de Limites de Mroute por Interface; Controle de Admissão no Link Agg-DSLAM



Exemplo 2 - Controle de admissão de entrada no link Agg-DSLAM

Em vez do limite "out" na interface de saída do dispositivo upstream, é possível usar limites RPF na interface RPF do dispositivo downstream. Isso efetivamente tem o mesmo resultado do exemplo anterior e pode ser útil se o dispositivo downstream não for um dispositivo Cisco IOS.

Fig 22: Uso de Limites de Mroute por Interface; Controle de Admissão de Entrada



Exemplo 3 - Limites baseados em largura de banda

Você pode fazer uma subdivisão adicional da largura de banda de acesso entre vários provedores de conteúdo e oferecer a cada provedor de conteúdo uma parcela justa da largura de banda no uplink para o DSLAM. Nesse caso, use o comando ip multicast limit cost:

<#root>

ip multicast limit cost

<ext-acl> <multiplier>

Com esse comando, é possível atribuir um "custo" (use o valor especificado em "multiplicador") a qualquer estado que corresponda à ACL estendida no limite de multicast ip.

Esse comando é global e vários custos simultâneos podem ser configurados.

Neste exemplo, é necessário suportar três provedores de conteúdo diferentes com acesso justo a

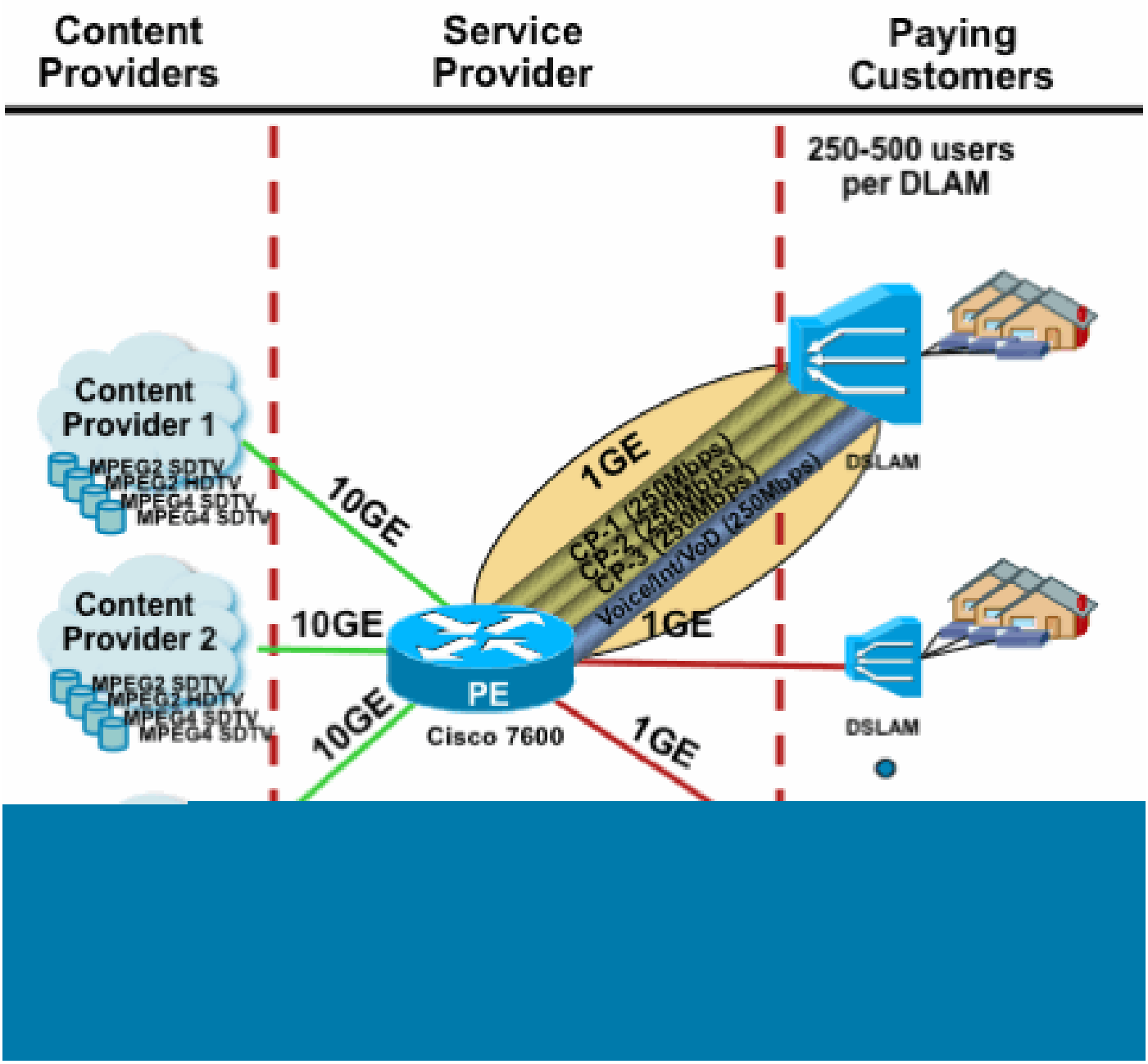
cada um na rede. Além disso, neste exemplo, é necessário oferecer suporte a fluxos MPEG (Moving Picture Experts Group) de vários tipos:

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

Nesse caso, você poderia alocar custos de largura de banda para cada tipo de fluxo e compartilhar o restante dos 750 Mbps entre os três provedores de conteúdo com esta configuração:

```
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
```

Fig 23: Fator de custo para limites de estado de Mroute por interface



Multicast e IPSec

Introdução ao GET VPN

Como ocorre com o unicast, o tráfego multicast também às vezes precisa ser protegido para fornecer confidencialidade ou proteção de integridade. Há duas áreas principais em que esses serviços podem ser necessários:

- Criptografia de fluxos multicast (por exemplo, em aplicativos bancários que transmitem dados confidenciais para um grande conjunto de receptores que usam multicast) - essa é a segurança do plano de dados.
- Criptografia de protocolos de plano de controle que usam multicast, OSPF ou PIM, por

exemplo - isso é segurança de plano de controle.

IPSec como um protocolo [RFCs 6040, 7619, 4302, 4303, 5282] é especificamente limitado ao tráfego unicast (por RFC). Lá, uma "associação de segurança" (SA) é estabelecida entre dois peers unicast. Para aplicar IPSec ao tráfego multicast, uma opção é encapsular o tráfego multicast dentro de um túnel GRE e, em seguida, aplicar IPSec ao túnel GRE, que é unicast. Uma abordagem mais recente usa uma única associação de segurança estabelecida entre todos os membros do grupo. O Domínio de Interpretação de Grupo (GDOI - Group Domain of Interpretation) [RFC 6407] define como isso é obtido.

Com base no GDOI, a Cisco desenvolveu uma tecnologia chamada de Transporte de Criptografia de Grupo (GET - Group Encryption Transport) VPN. Essa tecnologia usa o "Modo de túnel com preservação de endereço", conforme definido no documento "draft-ietf-msec-ipsec-extensions". No GET VPN, primeiro uma associação de segurança de grupo é estabelecida entre todos os membros do grupo. Subsequentemente, o tráfego é protegido, com ESP (encapsulated security payload) ou AH (authentication header), que usa o modo de túnel com preservação de endereço.

Em resumo, o GET VPN encapsula um pacote multicast que usa as informações de endereço do cabeçalho original e, em seguida, protege o pacote interno em relação à política de grupo, com um ESP, por exemplo.

A vantagem do GET VPN é que o tráfego multicast não é afetado de forma alguma pelos mecanismos de encapsulamento de segurança. Os endereços de cabeçalho IP roteados permanecem os mesmos do cabeçalho IP original. O tráfego multicast pode ser protegido da mesma maneira com ou sem GET VPN.

A política que é aplicada aos nós GET VPN é definida centralmente em um Servidor de Chave de Grupo e distribuída para todos os nós de grupo. Portanto, todos os nós do grupo têm a mesma política e as mesmas configurações de segurança aplicadas ao tráfego do grupo. Semelhante ao IPSec padrão, a política de criptografia define que tipo de tráfego precisa ser protegido de que maneira. Isso permite que o GET VPN seja usado para várias finalidades.

Use GET VPN para criptografar o tráfego de plano de dados multicast

A política de criptografia em toda a rede é definida no servidor de chave de grupo e distribuída para os terminais GET VPN. A política contém a política IPSec (modo IPSec - aqui: modo de túnel com preservação de cabeçalho) e os algoritmos de segurança a serem usados (por exemplo, AES). Ele também contém uma política que descreve qual tráfego pode ser protegido, conforme definido por uma ACL.

A VPN GET pode ser usada para tráfego multicast e unicast. Uma política para proteger o tráfego unicast poderia ser definida por uma ACL:

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

Isso criptografaria todo o tráfego com um IP de origem de 10/8 e um IP de destino de 10/8. Todo o tráfego restante, por exemplo, o tráfego de 10/8 para outro endereço, seria ignorado pelo GET VPN.

A aplicação de GET VPN para tráfego multicast é tecnicamente a mesma. Por exemplo, essa entrada de controle de acesso (ACE) pode ser usada para proteger o tráfego de qualquer origem para os respectivos grupos multicast:

```
permit ip any 239.192.0.0 0.0.255.255
```

Essa política corresponde a todas as origens ("qualquer") e a todos os grupos multicast que começam com 239.192. O tráfego para outros grupos multicast não é protegido.

Observação: deve-se prestar muita atenção à construção da ACL criptografada. O tráfego de gerenciamento, ou o tráfego que se origina fora do domínio GET VPN, mas termina dentro (ou seja, o tráfego que passa apenas por um ponto final de criptografia), deve ser excluído da política GDOI.

Os erros comuns incluem:

- permit ip any 224.0.0.0 0.255.255.255: Isso também criptografa o tráfego OSPF e outro tráfego do plano de controle, que é destinado a um roteador de mesmo nível, por exemplo.
- O tráfego de gerenciamento não é excluído da política de criptografia, que termina dentro da rede. Isso inclui o próprio tráfego GDOI.

Use GET VPN para autenticar o tráfego plano de controle

Geralmente, é uma prática recomendada autenticar o tráfego do plano de controle, como protocolos de roteamento, para garantir que as mensagens venham de um peer confiável. Isso é comparativamente simples para protocolos de plano de controle que usam unicast, como BGP. No entanto, muitos protocolos de plano de controle usam tráfego multicast. Exemplos são OSPF, RIP e PIM. Consulte IPv4 Multicast Address Space Registry da IANA para obter a lista completa.

Alguns desses protocolos têm autenticação integrada, como o Routing Information Protocol (RIP) ou o Enhanced Interior Group Routing Protocol (EIGRP), outros dependem do IPSec para fornecer essa autenticação (por exemplo, OSPFv3, PIM). Para o último caso, o GET VPN fornece uma maneira escalável de proteger esses protocolos. Na maioria dos casos, o requisito é a autenticação de mensagem de protocolo ou, em outras palavras, a verificação de que uma mensagem foi enviada por um peer confiável. No entanto, o GET VPN também permite a criptografia dessas mensagens.

Para proteger (geralmente autenticar apenas) esse tráfego de plano de controle, o tráfego precisa ser descrito com uma ACL e incluído na política GET VPN. Os detalhes dependem do protocolo a ser protegido, onde é necessário prestar atenção para se a ACL inclui o tráfego que passa

apenas um nó GET VPN de entrada (que é encapsulado), ou também um nó de saída.

Há duas maneiras fundamentais de proteger protocolos PIM:

- permit ip any 224.0.0.13 0.0.0.0: este é o grupo multicast "Todos os roteadores PIM". No entanto, isso não protege mensagens PIM unicast
- permit pim any any: Isso protege o protocolo PIM, independentemente de ser usado multicast ou unicast

---

Observação: os comandos são fornecidos como exemplos para ajudar a explicar um conceito. Por exemplo, é necessário excluir certos protocolos PIM usados para inicializar o PIM, como BSR ou AutoRP. Os métodos Noth têm certas vantagens e inconvenientes que dependem da implantação. Consulte a literatura específica sobre como proteger o PIM com GET VPN para obter detalhes.

Conclusões

O multicast é um serviço cada vez mais comum em redes. O surgimento de serviços de IPTV em redes de banda larga residenciais/residenciais e a mudança para aplicativos de comércio eletrônico em muitos dos mercados financeiros mundiais são apenas dois exemplos de requisitos que fazem do multicast um requisito absoluto. O multicast vem com uma variedade de diferentes desafios de configuração, operação e gerenciamento. Um dos principais desafios é a segurança.

Este documento examinou várias maneiras pelas quais o multicast pode ser protegido:

- Primeiro, observe o controle multicast geral e os planos de dados, uma explicação de como as diferenças do unicast apresentam novos desafios de segurança.
- Em seguida, um exame dos principais protocolos encontrados em uma rede multicast, em particular IGMP, PIM e MSDP, foi examinado com algum detalhe. Em cada caso, foi fornecida uma descrição das ameaças à segurança e as melhores práticas recomendadas para mitigação contra essas ameaças.
- Além disso, alguns exemplos específicos de como o multicast pode ser protegido em alguns aplicativos específicos, como redes de borda de banda larga, onde a largura de banda pode ser limitada em comparação com a quantidade de largura de banda que os fluxos de vídeo específicos podem exigir.
- Finalmente, a arquitetura GET VPN foi descrita como um meio de envio múltiplo integrado com IPSec para a entrega de VPNs seguras.

Com a segurança multicast em mente, lembre-se de como ela é diferente do unicast. A transmissão multicast é baseada na criação de estado dinâmico, o multicast envolve a replicação dinâmica de pacotes e o multicast cria árvores unidirecionais em resposta às mensagens PIM JOIN / PRUNE. A segurança de todo esse ambiente envolve a compreensão e a implantação de uma estrutura rica de comandos IOS Cisco. Esses comandos estão amplamente centralizados na proteção de operações de protocolo, estados (multicast) ou vigilantes colocados contra pacotes como CoPP. Com o uso correto desses comandos é possível fornecer um serviço protegido

robusto para multicast IP.

Em resumo, há várias abordagens que são promovidas e descritas neste documento:

1. Uso difundido de SSM - este é o modo PIM mais simples que também permite o uso de encaminhamento (S,G).
2. Se forem necessários serviços ASM, assegure-se de que um serviço robusto possa ser fornecido - o uso de RPs definidos estaticamente fornece um plano de controle mais seguro do que os anúncios RP dinâmicos. O RP automático e o BSR são mais flexíveis
3. Se o PIM-SM estiver ativado, observe as áreas de vulnerabilidade específica, como o túnel de registro para o RP, e assegure-se de que o DR esteja sempre bem protegido. A CoPP é muito útil nessas áreas.
4. Se forem necessários serviços ASM entre domínios, considere se o BiDir PIM pode ser implantado.
5. Usar limites globais de estado mroute/igmp - entender os recursos de suas plataformas juntamente com a quantidade máxima esperada de estado que você precisa em circunstâncias normais e no pior cenário possível. Configure limites dentro dos recursos da sua plataforma que permitam que a sua rede opere até os limites máximos.
6. Filtros fundamentais - rACL/CoPP e ACLs de infraestrutura, que bloqueiam o PIM na camada de acesso

O Multicast IP é um meio estimulante e escalável de oferecer uma variedade de serviços de aplicativos. Como o unicast, ele precisa ser protegido em várias áreas diferentes. Este documento fornece os componentes básicos que podem ser usados para proteger uma rede multicast IP.

Informações Relacionadas

- Diretrizes para Alocação de Endereço Multicast IP Empresarial
- Configurar filtros IGMP IPv4
- Group Encrypted Transport VPN

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.