Déploiements de multidiffusion IP sécurisée

Contenu

Introduction

Ce document décrit les conseils généraux sur les meilleures pratiques pour sécuriser une infrastructure réseau de multidiffusion IP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- multicast IP

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document couvre certains concepts de base, la terminologie et traite des rubriques répertoriées :

- Mécanismes permettant de sécuriser une plate-forme spécifique et le réseau en général.
- Tous les modèles ASM (Source Multicast) et SSM (Source Specific Multicast).
- Sécurité de réseau privé virtuel multidiffusion (MVPN).
- Architecture de réseau privé virtuel (VPN) GET (Group Encrypted Transport) qui assure la confidentialité et l'intégrité du trafic du plan de données ou du plan de contrôle multicast.

Terminologie

Dans la multidiffusion IP, il existe deux modèles de service classiques :

1. Toute multidiffusion source (ASM)

2. Multidiffusion spécifique à la source (SSM)

Dans ASM, le récepteur rejoint un groupe G via un rapport d'adhésion IGMP (Internet Group Membership Protocol) ou MLD (Multicast Listener Discovery) pour indiquer le groupe. Ce rapport demande le trafic envoyé par n'importe quelle source au groupe G, d'où le nom « any source ». En revanche, en SSM, le récepteur rejoint un canal spécifique défini par une source S, qui envoie vers un groupe G. Chacun de ces modèles de service est décrit en détail ci-après.

Toute multidiffusion source

Le modèle ASM se caractérise par deux classes de protocoles : «dense mode flood-and-prune» et «sparse mode explicit join» :

i) Protocoles Dense Mode Flood-and-Prune (DVMRP / MOSPF / PIM-DM)

Dans les protocoles en mode dense, tous les routeurs du réseau connaissent toutes les arborescences, leurs sources et leurs récepteurs. Des protocoles tels que DVMRP (Distance Vector Multicast Routing Protocol) et PIM (Protocol Independent Multicast) en mode dense diffusent des informations de « source active » sur l'ensemble du réseau et créent des arborescences via la création de « Prune State » dans des parties de la topologie où le trafic d'une arborescence spécifique est indésirable. Ils sont également appelés protocoles d'inondation et de élagage. Dans le protocole MOSPF (Multicast Open Shortest Path First), les informations sur les récepteurs sont diffusées sur l'ensemble du réseau pour prendre en charge la création d'arbres.

Les protocoles en mode dense ne sont pas souhaitables, car chaque arborescence créée dans une partie du réseau peut toujours entraîner une utilisation des ressources (avec un impact sur la convergence) sur tous les routeurs du réseau (ou dans la portée administrative, si elle est configurée). Ces protocoles ne sont pas abordés plus en détail dans la suite de cet article.

ii) Protocoles de jointure explicite en mode dispersé (PIM-SM/PIM-BiDir)

Avec les protocoles de jointure explicite en mode clairsemé, les périphériques ne créent pas d'état spécifique au groupe dans le réseau, à moins qu'un récepteur n'ait envoyé un rapport d'appartenance IGMP/MLD explicite (ou « jointure ») pour un groupe. Cette variante de l'ASM est bien connue pour évoluer et constitue le paradigme de mise au point multicast.

C'est la base du mode PIM-Sparse, que la plupart des déploiements de multidiffusion ont utilisé jusqu'à présent. C'est aussi la base de la PIM bidirectionnelle (PIM-BiDir), qui est de plus en plus déployée pour de NOMBREUSES (sources) à de NOMBREUSES (récepteurs) applications.

Ces protocoles sont appelés mode intermédiaire, car ils prennent efficacement en charge les arborescences de diffusion multidiffusion IP avec une population de récepteurs « éparses » et créent un état de plan de contrôle uniquement sur les routeurs sur le chemin entre les sources et les récepteurs, et dans PIM-SM/BiDir, le point de rendez-vous (RP). Ils ne créent jamais d'état dans d'autres parties du réseau. L'état d'un routeur est construit explicitement uniquement lorsqu'il

reçoit une jointure d'un routeur ou d'un récepteur en aval, d'où le nom de « protocoles de jointure explicites ».

PIM-SM et PIM-BiDir utilisent des « ARBORESCENCES PARTAGÉES », qui permettent au trafic provenant de n'importe quelle source d'être transmis à un récepteur. L'état de multidiffusion sur une arborescence partagée est appelé état (*, G), où * est un caractère générique pour TOUTE SOURCE. En outre, PIM-SM prend en charge la création d'états liés au trafic d'une source spécifique. On les appelle ARBRES SOURCE et l'état associé est appelé état (S, G).

Multidiffusion spécifique à la source

SSM est le modèle utilisé lorsque le récepteur (ou un proxy) envoie (S, G) « joint » pour indiquer qu'il veut recevoir le trafic envoyé par la source S au groupe G. Cela est possible avec les rapports d'appartenance en mode « INCLUDE » IGMPv3/MLDv2. Ce modèle est appelé modèle SSM (Source-Specific Multicast). SSM impose l'utilisation d'un protocole de jointure explicite entre les routeurs. Le protocole standard pour cela est PIM-SSM, qui est simplement le sous-ensemble de PIM-SM utilisé pour créer des arborescences (S, G). Il n'existe aucun état d'arborescence partagée (*, G) dans SSM.

Les récepteurs multidiffusion peuvent ainsi « rejoindre » un groupe ASM G, ou « rejoindre » (ou plus précisément « s'abonner » à) un canal SSM (S, G). Pour éviter la répétition du terme « groupe ASM ou canal SSM », on utilise le terme flux (multicast), ce qui implique que le flux pourrait être un groupe ASM ou un canal SSM.

Protocoles de multidiffusion/types de paquets pertinents

Pour sécuriser un réseau de multidiffusion, il est important de comprendre les types de paquets couramment rencontrés et comment les protéger. Il y a trois principaux protocoles qui doivent être concernés :

1. IGMP / MLD
2. PIM
3. MSDP

Dans la section suivante, chacun de ces protocoles est traité et les problèmes qui peuvent survenir avec chacun d'eux, respectivement.

Paquets IGMP / MLD

IGMP / MLD est le protocole utilisé par les récepteurs de multidiffusion pour signaler à un routeur qu'ils souhaitent recevoir du contenu pour un groupe de multidiffusion particulier. Le protocole IGMP (Internet Group Membership Protocol) est le protocole utilisé dans IPv4 et le protocole MLD (Multicast Listener Discovery) est le protocole utilisé dans IPv6.

Deux versions d'IGMP sont couramment déployées, IGMPv2 et IGMPv3. Deux versions de MLD

sont également couramment déployées, MLDv1 et MLDv2.

IGMPv2 et MLDv1 sont fonctionnellement équivalents, et IGMPv3 et MLDv2 sont fonctionnellement équivalents.

Ces protocoles sont spécifiés dans les liens suivants :

IGMPv2 : RFC 2236

MLDv1 : RFC 3590

IGMPv3 et MLDv2 : RFC 4604

IGMPv2 et IGMPv3 sont non seulement un protocole, mais également un protocole IPv4 (en particulier, le protocole numéro 2). Il est non seulement utilisé comme décrit dans ces documents RFC pour signaler l'appartenance à un groupe de multidiffusion, mais également par d'autres protocoles de multidiffusion IPv4 tels que DVMRP, PIM version 1, mtrace et mrinfo. Il est important de se souvenir de cela lorsque vous tentez de filtrer IGMP (via des ACL Cisco IOS®, par exemple). Dans IPv6, MLD n'est pas un protocole IPv6 ; à la place, ICMPv6 est utilisé pour transporter les paquets MLD. PIM version 2 est le même type de protocole dans IPv4 et IPv6 (numéro de protocole 103).

Paquets de contrôle PIM

Cette section traite des paquets de contrôle PIM de multidiffusion et de monodiffusion. L'Auto-RP ainsi que le routeur d'amorçage (BSR), qui sont des moyens de sélectionner des points de rendez-vous et de contrôler les affectations de groupe à RP dans les réseaux PIM-SM, sont abordés.

Paquets de contrôle PIM multidiffusion

Les paquets de contrôle PIM multidiffusion incluent :

- **PIM Hello** : le paquet PIM Hello est un paquet de multidiffusion IP à étendue link-local envoyé à un routeur connecté au même réseau pour établir des voisins PIM.
- **Jonction/élagage PIM** - Les jonctions/élagages PIM sont des paquets de multidiffusion IP d'étendue link-local envoyés pour créer/supprimer l'état de multidiffusion et sont envoyés uniquement aux voisins PIM. Ils sont multidiffusés au sein du LAN pour faciliter l'assertion, la suppression des rapports et d'autres détails du protocole PIM, mais ils sont toujours dirigés vers un voisin spécifique.
- **PIM DF-elect** - PIM Designated Forwarder est le routeur PIM bidirectionnel responsable des (*, G) JOINS envoyés au RP pour le compte des récepteurs connectés ou des voisins PIM en aval. Dans les cas où un routeur PIM détecte un autre routeur qui envoie (*, G) JOINS sur le même segment pour le même groupe G, il y a une sélection pour déterminer le routeur avec le meilleur chemin vers le RP.
- **Assertion PIM** - Les assertions PIM sont des paquets multicast IP link-local envoyés lorsqu'un routeur PIM connecté à un segment de réseau qui transfère activement des paquets pour une interface particulière (S, G) à partir d'une interface particulière commence à RECEVOIR des

paquets pour cette même interface (S, G) sur la même interface sur laquelle sont transférés. Cet événement indique la présence d'un autre routeur qui pense qu'il s'agit du Single Forwarder (SF) pour ce routeur (S, G). Le mécanisme Assert sélectionne un SF unique pour cela (S, G). Le routeur PIM SF est choisi pour transférer des paquets pour un flux particulier (S, G). Le protocole PIM permet à différents routeurs d'exécuter le rôle de SF pour le compte de différents (S, G). Idéalement, il n'y a qu'un seul SF par (S, G). Ne confondez pas le routeur SF et le routeur désigné. Le routeur désigné PIM est le routeur responsable de JOIN / PRUNES ou SOURCE REGISTERS qui sont envoyés au RP dans un réseau PIM-SM.
- **PIM Bootstrap** - Les messages de démarrage PIM sont envoyés dans un réseau PIMv2 pour faciliter la sélection dynamique d'un point de rendez-vous pour un groupe G particulier.

Paquets de contrôle PIM monodiffusion

Les paquets de contrôle PIM monodiffusion sont dirigés vers ou depuis le RP et incluent :

- **Paquet du registre source** - Les paquets du registre source PIM sont envoyés pour enregistrer une nouvelle source de multidiffusion avec un point de rendez-vous. Dès qu'une source commence à envoyer des paquets de multidiffusion, le routeur désigné qui est connecté au réseau source envoie un flux de registre de monodiffusion au RP pour indiquer qu'il y a une source active présente pour un groupe de multidiffusion dont le RP est responsable.
  Les paquets du registre source sont envoyés en tant qu'encapsulation monodiffusion du flux multidiffusion d'origine.
  Les messages de registre PIM sont commutés au niveau du processus et sont envoyés uniquement jusqu'à ce que le RP envoie un message d'arrêt de registre. L'impact de ces paquets sur les performances est proportionnel au débit de la source (par flux (S, G)).
- **Register Stop Packet** : les paquets d'arrêt de l'enregistrement PIM sont envoyés du point de rendez-vous au DR PIM qui a envoyé le message d'enregistrement. Les messages d'arrêt de l'enregistrement sont envoyés dès que le RP commence à recevoir des paquets de multidiffusion nativement de la source.
- **BSR Candidate-Rendezvous Point Advertisement Packet** - PIM BSR C-RP-Advertisement Packets envoyés au BSR pour annoncer un candidat RP une fois que le BSR est élu.

Figure 1 : Paquets de monodiffusion PIM

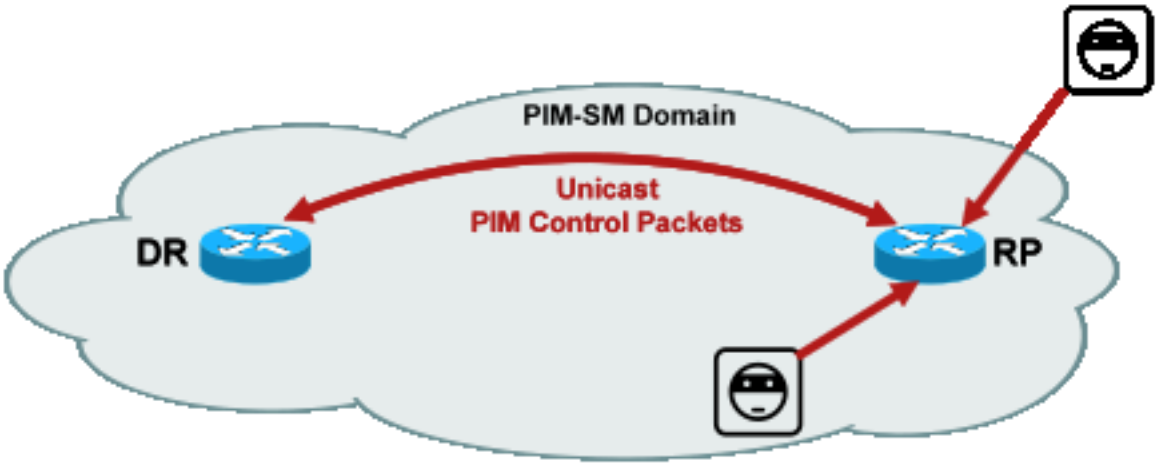

Fig1

_PIM_unicast

Les attaques qui exploitent ces paquets peuvent provenir de n'importe où, car ces paquets sont en monodiffusion.

Paquets Auto-RP

Auto-RP est un protocole développé par Cisco qui sert le même objectif que PIMv2 BSR. Auto-RP a été développé avant BSR, et prend uniquement en charge IPv4. BSR prend en charge IPv4 et IPv6. L'agent de mappage dans Auto-RP sert la même fonction que le routeur d'amorçage dans BSR. Dans BSR, les messages du C-RP sont monodiffusés au routeur bootstrap. Dans Auto-RP, les messages sont envoyés via la multidiffusion à l'agent de mappage, ce qui permet des filtres plus faciles à la frontière, comme décrit plus loin. L'Auto-RP est décrit en détail dans ce lien : https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Dans Cisco IOS, les paquets AutoRP/BSR sont toujours transférés et ne sont actuellement pas désactivés. Cela peut présenter une exposition de sécurité particulière dans le cas de l'Auto-RP.

Figure 2 : Paquets Auto-RP

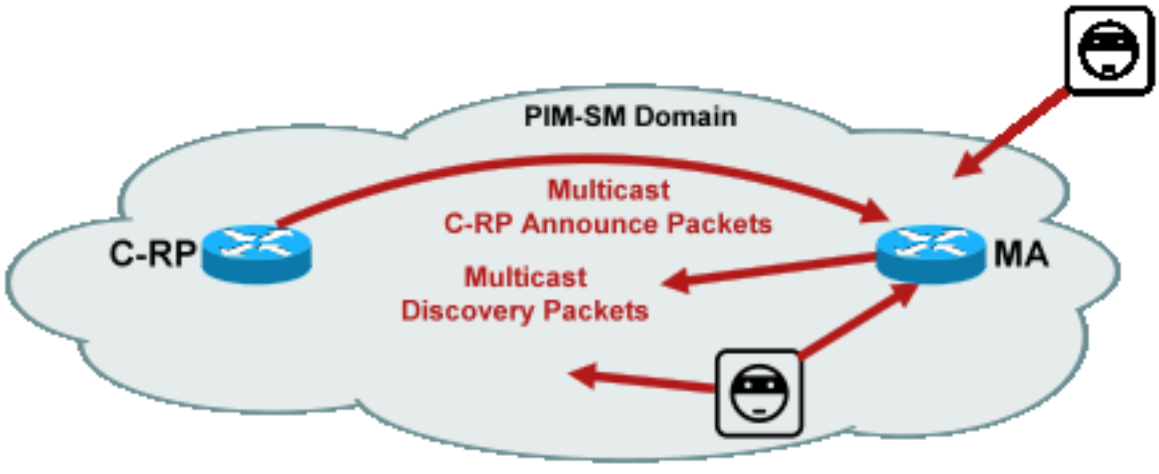

Fig2_A

utoRP_packets

Note: Même si Auto-RP est utilisé comme mécanisme pour l'annonce et la découverte PIM-SM RP, il n'utilise pas les paquets PIM (protocole IP 103) ; à la place, il utilise les paquets du port 496 du protocole UDP (User Datagram Protocol) avec des adresses de multidiffusion.

Il existe deux types de paquets utilisés par Auto-RP :

- C-RP-Announce packets : ces paquets sont multidiffusés vers tous les agents de mappage et utilisent une adresse « bien connue » réservée à l'IANA (Internet Assigned Numbers Authority) (224.0.1.39). Ils sont envoyés par un C-RP pour annoncer l'adresse RP et la plage de groupes pour lesquels ce RP peut agir en tant que RP.
- Paquets de détection C-RP : ces paquets sont multidiffusés vers tous les routeurs PIM et utilisent une adresse « bien connue » réservée par l'IANA (224.0.1.40). Ils sont envoyés par l'agent de mappage Auto-RP pour annoncer le C-RP spécifique qui est sélectionné comme RP pour une plage de groupe particulière.

Chacun de ces types de paquets est destiné à être diffusé sur le réseau.

Dans Cisco IOS, les adresses 224.0.1.39 et 224.0.1.40 sont toutes deux transmises en mode dense PIM pour éviter un problème d'absence de connaissance préalable du RP pour un groupe lorsque ce groupe est utilisé pour distribuer des informations RP. C'est la seule utilisation recommandée du mode dense PIM.

Dans Cisco IOS XR, les messages Auto-RP sont inondés de RPF (Reverse Path Forwarding) saut par saut de voisin à voisin. Par conséquent, il n'est pas nécessaire de créer un état Mroute PIM DM pour prendre en charge Auto-RP dans Cisco IOS XR. En fait, Cisco IOS XR ne prend pas du tout en charge PIM-DM.

Paquets MSDP (Multicast Service Discovery Protocol)

MSDP est le protocole IPv4 qui permet à une source d'un domaine d'être annoncée à un récepteur d'un autre domaine via leurs points de rendez-vous respectifs. Le protocole MSDP est spécifié dans la RFC 3618.

Afin de partager des informations sur les sources actives entre les domaines PIM, MSDP est utilisé. Si une source devient active dans un domaine, alors MSDP s'assure que tous les domaines homologues apprennent cette nouvelle source en temps opportun, ce qui permet aux récepteurs dans d'autres domaines d'entrer rapidement en contact avec cette nouvelle source s'il s'avère qu'elle a été envoyée à un groupe dans lequel les récepteurs ont un intérêt. MSDP est nécessaire pour les communications multidiffusion ASM / PIM-SM et s'exécute sur une connexion TCP (Transport Control Protocol) monodiffusion configurée entre les points de rendez-vous dans les domaines respectifs.

Menaces dans un environnement multidiffusion

Zones de confiance et limites de confiance

Cette section du document est organisée par entités fonctionnelles dans le réseau. Le modèle de

menace présenté est conçu autour de ces entités. Par exemple, ce document explique comment un routeur dans un réseau de multidiffusion peut être sécurisé (d'un point de vue de multidiffusion), indépendamment de l'endroit où le routeur est déployé. De même, il existe des considérations sur la façon de déployer des mesures de sécurité à l'échelle du réseau, ou des mesures sur un routeur désigné, un point de rendez-vous, etc

Les menaces décrites ici suivent également cette logique et sont organisées par fonction logique du réseau.

Présentation des menaces

Au niveau abstrait, tout déploiement de multidiffusion peut être sujet à un certain nombre de menaces sur divers aspects de la sécurité. Les aspects clés de la sécurité sont la confidentialité, l'intégrité et la disponibilité.

- **Menaces contre la confidentialité** : Dans la plupart des applications, le trafic de multidiffusion n'est pas chiffré et peut donc être écouté ou capturé sur n'importe quelle ligne ou élément réseau du chemin. Dans la section consacrée à GET VPN, les méthodes de cryptage du trafic multidiffusion pour empêcher de telles attaques sont abordées.
- **Menaces contre l'intégrité du trafic** : En l'absence de sécurité au niveau des applications ou de sécurité réseau, telle que GET VPN, le trafic de multidiffusion est vulnérable aux modifications en transit. Ceci est particulièrement important pour le trafic du plan de contrôle qui utilise la multidiffusion, comme OSPF, PIM et de nombreux autres protocoles.
- **Menaces contre l'intégrité du réseau** : Sans les mécanismes de sécurité décrits dans ce document, les expéditeurs, les récepteurs non autorisés ou les éléments réseau compromis peuvent accéder au réseau de multidiffusion, envoyer et recevoir du trafic sans autorisation (vol de service) ou surcharger les ressources réseau.
- **Menaces contre la disponibilité** : Il existe un certain nombre de possibilités d'attaque par déni de service qui peuvent rendre les ressources indisponibles pour les utilisateurs légitimes.

Les sections suivantes traitent des menaces pour chaque fonction logique du réseau.

Menaces de base contre un routeur

Il existe un certain nombre de menaces fondamentales contre un routeur, qu'il prenne en charge ou non la multidiffusion et que l'attaque implique un trafic ou des protocoles de multidiffusion.

Les attaques par déni de service (DoS) sont les vecteurs d'attaque génériques les plus importants dans un réseau. En principe, chaque élément du réseau peut être la cible d’une attaque DoS, qui peut surcharger l’élément et entraîner une perte ou une dégradation de service pour les utilisateurs légitimes. Il est primordial de suivre les recommandations de base en matière de sécurité réseau qui s'appliquent à la monodiffusion.

Il convient de noter que les attaques multidiffusion ne sont pas toujours intentionnelles, mais

souvent accidentelles. Par exemple, le ver Witty, observé pour la première fois en mars 2004, est un exemple de ver qui se propage par des attaques aléatoires sur des adresses IP. En raison de la randomisation complète de l'espace d'adressage, les destinations IP de multidiffusion ont également été affectées par le ver. Dans de nombreuses entreprises, un certain nombre de routeurs de premier saut se sont effondrés parce que le ver a envoyé des paquets à plusieurs adresses de destination de multidiffusion différentes. Cependant, les routeurs n'étaient pas adaptés à une telle charge de trafic de multidiffusion avec l'état de création associé et ont effectivement connu un épuisement des ressources. Cela illustre la nécessité de sécuriser le trafic de multidiffusion, même si la multidiffusion n'est pas utilisée dans une entreprise.

Les menaces génériques contre les routeurs incluent :

- Inondations de paquets de tout type ; par exemple, contre les chemins matériels tels que les chemins lents (punt) et les chemins logiciels tels que les ports du plan de gestion ou de contrôle, qui incluent Secure Shell (SSH), Telnet, Border Gateway Protocol (BGP), OSPF, Network Time Protocol (NTP), etc
- Intrusions dans le routeur, avec exploitation ultérieure des fonctions sur le routeur ; Les mots de passe Telnet ou SSH faibles et les chaînes de communauté SNMP (Simple Network Management Protocol) faibles sont un problème courant dans les réseaux modernes.
- Des problèmes opérationnels tels que des erreurs de configuration ou des attaques internes peuvent compromettre la sécurité de l'ensemble du réseau et de son trafic.

Lorsque la multidiffusion est activée sur un routeur, elle doit être sécurisée en plus de la monodiffusion. L'utilisation de la multidiffusion IP ne modifie pas le modèle de menace fondamental ; cependant, il permet des protocoles supplémentaires (PIM, IGMP, MLD, MSDP) qui pourraient être sujets à des attaques, qui doivent être sécurisées spécifiquement. Lorsque le trafic de monodiffusion est utilisé dans ces protocoles, le modèle de menace est identique aux autres protocoles exécutés par le routeur.

Il est important de noter que le trafic de multidiffusion ne peut pas être utilisé de la même manière que le trafic de monodiffusion pour attaquer un routeur, car le trafic de multidiffusion est fondamentalement « axé sur le récepteur » et ne peut pas être ciblé sur une destination distante. Une cible d'attaque doit être explicitement « jointe » au flux de multidiffusion. Dans la plupart des cas (l'exception Auto-RP est la principale), les routeurs écoutent et reçoivent uniquement le trafic de multidiffusion « link-local ». Le trafic local de la liaison n'est jamais transféré. Par conséquent, les attaques sur un routeur avec des paquets de multidiffusion ne peuvent provenir que d'attaquants directement connectés.

Menaces du côté source

Les sources de multidiffusion, qu'il s'agisse de PC ou de serveurs vidéo, ne sont parfois pas sous le même contrôle administratif que le réseau. Par conséquent, l'expéditeur est généralement considéré comme non fiable, du point de vue de l'opérateur réseau. Étant donné les puissantes capacités des PC et des serveurs, ainsi que leurs paramètres de sécurité complexes, souvent incomplets, les expéditeurs représentent une menace importante contre tout réseau, y compris la multidiffusion. Ces menaces incluent :

- **Attaques de couche 2 :** il existe une large gamme de formes d'attaque sur la couche 2 pour effectuer divers types d'attaques. Elles s'appliquent à la monodiffusion et à la multidiffusion. Comme ces formes d'attaque ne sont pas spécifiques à la multidiffusion, elles ne sont pas traitées plus en détail dans ce document. Pour plus d'informations, reportez-vous au livre de presse Cisco « LAN Switch Security », ISBN-10: 1-58705-467-1 .
- **Attaques avec trafic de multidiffusion :** comme décrit précédemment, il est difficile de mener des attaques avec trafic de multidiffusion car le routeur de premier saut ne transmet pas le trafic de multidiffusion à moins qu'il n'y ait un écouteur pour le groupe. Cependant, le premier saut peut être attaqué de différentes manières avec des paquets de multidiffusion :
- Attaques de saturation du réseau : Un pirate peut inonder un segment avec des paquets de multidiffusion, sur l'utilisation de la bande passante disponible, ce qui peut entraîner une condition de déni de service.
- Attaques d'état multidiffusion : Le routeur de premier saut est inondé de paquets de multidiffusion, ce qui peut créer un état trop important et une condition d'attaque DoS conséquente.
- Un expéditeur peut tenter de devenir le DR PIM, via les HELLO PIM qui sont envoyés. Dans ce cas, aucun trafic ne serait transféré vers ou depuis le LAN.
- Les paquets de sélection PIM DF pour un BiDir-PIM DF peuvent être usurpés. Dans ce cas, aucun trafic ne serait transféré vers ou depuis le LAN.
- Un expéditeur peut usurper des messages de détection de RP AutoRP ou de bootstrap BSR. Cela annoncerait effectivement un faux RP, et arrêterait ou perturberait un service PIM-SM/BiDir.
- Un expéditeur peut envoyer des attaques de monodiffusion, telles que des messages PIM source register/register-stop, ou peut envoyer des paquets BSR announce et annoncer un faux BSR.
- Un expéditeur peut envoyer des données à n'importe quel groupe de multidiffusion valide, sauf si ce dernier est filtré. Si une adresse source est usurpée et n'est pas empêchée à la périphérie, l'expéditeur peut utiliser l'adresse IP source d'un expéditeur légitime et remplacer le contenu dans certaines parties du réseau.
- Attaques multidiffusion contre les protocoles du plan de contrôle : Un certain nombre de protocoles non associés à la multidiffusion, tels que OSPF et DHCP (Dynamic Host Configuration Protocol), utilisent des paquets de multidiffusion, qui peuvent être utilisés pour attaquer ces protocoles
- **Inquisition :** il existe un certain nombre de formes d'attaque où un expéditeur peut prétendre être un autre expéditeur. Les adresses IP source usurpées sont l'une de ces formes d'attaque.
- **Vol de service :** sauf si les expéditeurs sont contrôlés, il est possible d'utiliser le service de multidiffusion de manière illégitime du côté de l'expéditeur.

> **Note**: Normalement, les hôtes n'envoient pas ou ne reçoivent pas de paquets PIM. L’hôte qui effectue cette opération peut probablement tenter une attaque.

Menaces du côté du destinataire

Le récepteur est également généralement une plate-forme dotée d'une puissance et d'une bande passante CPU importantes, et permet un certain nombre de formes d'attaque. Elles sont généralement identiques aux menaces du côté de l'expéditeur. Les attaques de couche 2 restent un vecteur d’attaque important. Les faux récepteurs et le vol de service sont également possibles

côté récepteur, sauf que le vecteur d'attaque est généralement IGMP (ou attaques de couche 2, comme mentionné).

Menaces contre un point de rendez-vous et BSR

Les RP PIM-SM et les BSR PIM sont des points critiques dans un réseau de multidiffusion et sont donc des cibles précieuses pour un attaquant. Lorsque le routeur de premier saut ne l'est pas non plus, seules les formes d'attaque de monodiffusion, qui incluent la monodiffusion PIM, peuvent être ciblées directement contre ces éléments. Les menaces contre les RP et les BSR incluent :

- Toutes les formes d'attaque génériques, comme décrit dans la section « Menaces de base contre un routeur ».
- Les attaques de monodiffusion PIM, potentiellement avec des adresses IP source usurpées, permettent des attaques par déni de service (DoS), via des messages PIM register ou register-stop envoyés par un périphérique malveillant.

Sécurité multidiffusion et monodiffusion (comparée)

Considérations / Filtres

Examinez la topologie de la Figure 3, qui présente une source, trois récepteurs (A, B, C), un commutateur (S1) et deux routeurs (R1 et R2). La ligne bleue représente un flux de monodiffusion et la ligne rouge un flux de multidiffusion. Les trois récepteurs sont membres du flux de multidiffusion.

Figure 3 : Réplication dans les routeurs et les commutateurs

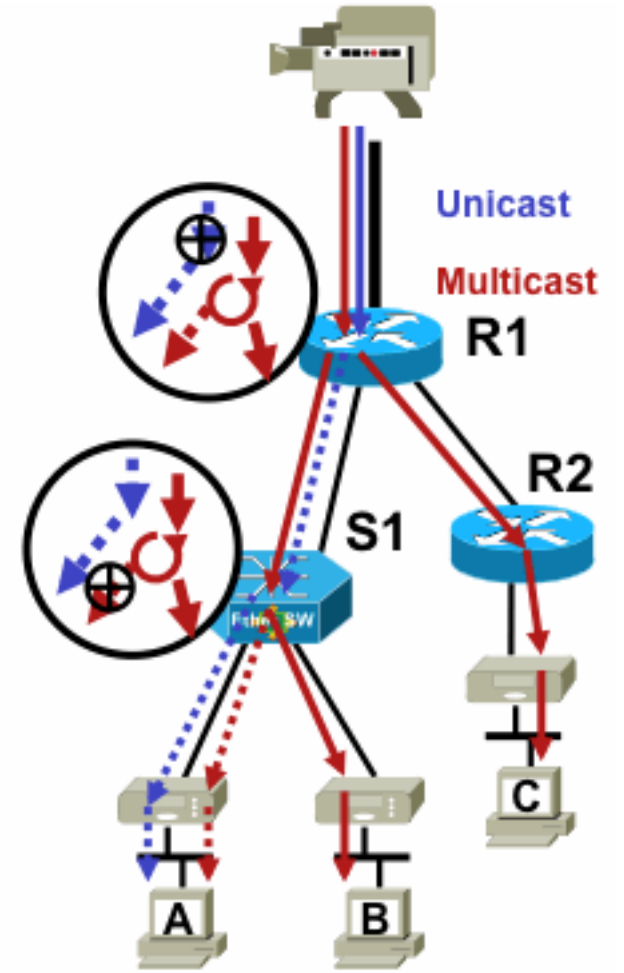

Fig3_replication_RS

Pour empêcher le flux de trafic d'une source spécifique vers un récepteur spécifique :

- Pour le flux de monodiffusion, installez un filtre n'importe où sur le chemin de l'expéditeur au destinataire.
- Pour le flux de multidiffusion, cependant, les administrateurs doivent être plus précis sur l'emplacement des filtres : au niveau du filtre côté récepteur après le dernier point de réplication avant le récepteur ; au niveau du filtre côté source avant le premier point de réplication après la source.

Attaques provenant de sources multidiffusion

Cette section s'applique aux modèles de service ASM et SSM, où le trafic est transféré en fonction de la réception de jointures explicites côté récepteur.

Pour les flux monodiffusion, il n'y a pas de protection de récepteur implicite. Une source de monodiffusion peut envoyer du trafic vers une destination, même si cette destination n'a pas demandé le trafic. Par conséquent, les mécanismes de défense tels que les pare-feu sont généralement utilisés pour protéger les terminaux. Par contre, la multidiffusion intègre une certaine protection implicite dans les protocoles. Idéalement, le trafic atteint uniquement un récepteur qui a rejoint le flux en question.

Avec ASM, les sources peuvent lancer l'insertion de trafic ou des attaques DoS par transmission de trafic de multidiffusion vers n'importe quel groupe pris en charge par un RP actif. Idéalement, ce trafic n'atteint pas un récepteur, mais peut atteindre au minimum le routeur de premier saut sur le chemin, ainsi que le RP, ce qui permet des attaques limitées. Toutefois, si une source malveillante connaît un groupe auquel un destinataire cible est intéressé et si aucun filtre approprié n’est en place, elle peut envoyer du trafic à ce groupe. Ce trafic est reçu tant que les récepteurs écoutent le groupe.

Avec SSM, les attaques par des sources indésirables ne sont possibles que sur le routeur de premier saut où le trafic s'arrête si aucun récepteur n'a rejoint ce canal (S, G). Cela n'entraîne aucune attaque d'état sur le routeur de premier saut, car il rejette tout le trafic SSM pour lequel aucun état de jointure explicite n'existe de la part des récepteurs. Dans ce modèle, il ne suffit pas qu'une source malveillante sache à quel groupe une cible est intéressée, car les « jointures » sont spécifiques à la source. Ici, les adresses IP source qui sont usurpées ainsi que les attaques de routage potentielles sont nécessaires pour réussir.

Attaques d'État

Même sans récepteurs présents dans un réseau, PIM-SM crée un état (S, G) et (*, G) sur le routeur de premier saut le plus proche de la source et également sur le point de rendez-vous. Il existe donc la possibilité d'une attaque d'état sur le réseau au niveau du routeur de premier saut source et sur le RP PIM-SM.

Si une source malveillante commence à envoyer du trafic à plusieurs groupes, alors pour chacun des groupes qui sont détectés, les routeurs dans le réseau créent l'état à la source et au RP, à condition que les groupes en question soient autorisés par la configuration du RP.

Par conséquent, PIM-SM est sujet à des attaques d'état et de trafic par des sources. L'attaque peut être aggravée si la source change son adresse IP source de manière aléatoire dans le préfixe correct, ou en d'autres termes, seuls les bits d'hôte de l'adresse sont usurpés.

Figure 4 : Attaques ASM RP

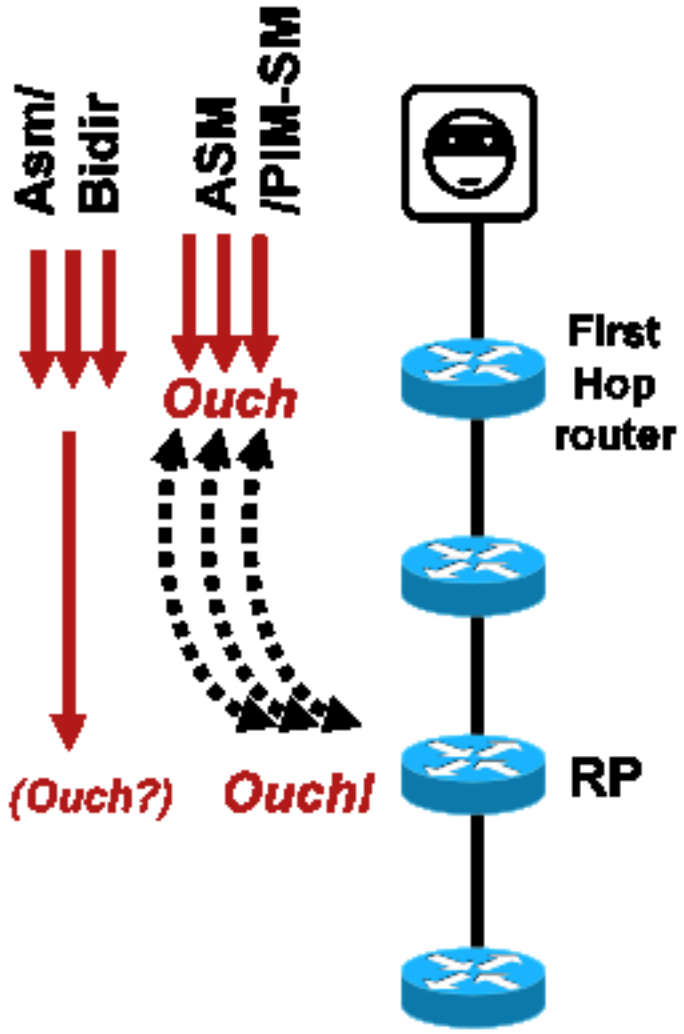

Fig4_ASM_RP_Attacks

Comme avec PIM-SSM, les attaques de création d'état PIM-BiDir à partir de sources sont impossibles. Le trafic dans PIM-BiDir est transféré sur l'état créé par les jointures des récepteurs ainsi que sur le trafic transféré d'état au RP, de sorte qu'il peut atteindre les récepteurs derrière le RP, puisque les jointures vont seulement au RP. Le trafic d'état à transfert vers le RP est appelé état (*, G/M) et est créé par la configuration du RP (statique, Auto-RP, BSR). Il ne change pas en présence de sources. Par conséquent, les pirates peuvent envoyer du trafic de multidiffusion à un RP PIM-BiDir, mais contrairement à PIM-SM, un RP PIM-BiDir n'est pas une entité « active » et se contente de transférer ou d'abandonner le trafic pour les groupes PIM-BiDir.

> **Note**: Sur certaines plates-formes Cisco IOS (*, G/M), l'état n'est pas pris en charge. Dans ce cas, les sources peuvent attaquer le routeur par transmission de trafic multidiffusion vers plusieurs groupes PIM-BiDir, ce qui entraîne la création d'un état (*, G). Par exemple, le commutateur Catalyst 6500 ne prend pas en charge les états (*, G/M).

Attaques lancées par le récepteur

Les attaques peuvent provenir de récepteurs de multidiffusion. Tout récepteur qui envoie un rapport IGMP/MLD crée généralement un état sur le routeur de premier saut. Il n'existe pas de mécanisme équivalent en monodiffusion.

Figure 5 : Transfert de trafic basé sur la jointure explicite côté récepteur

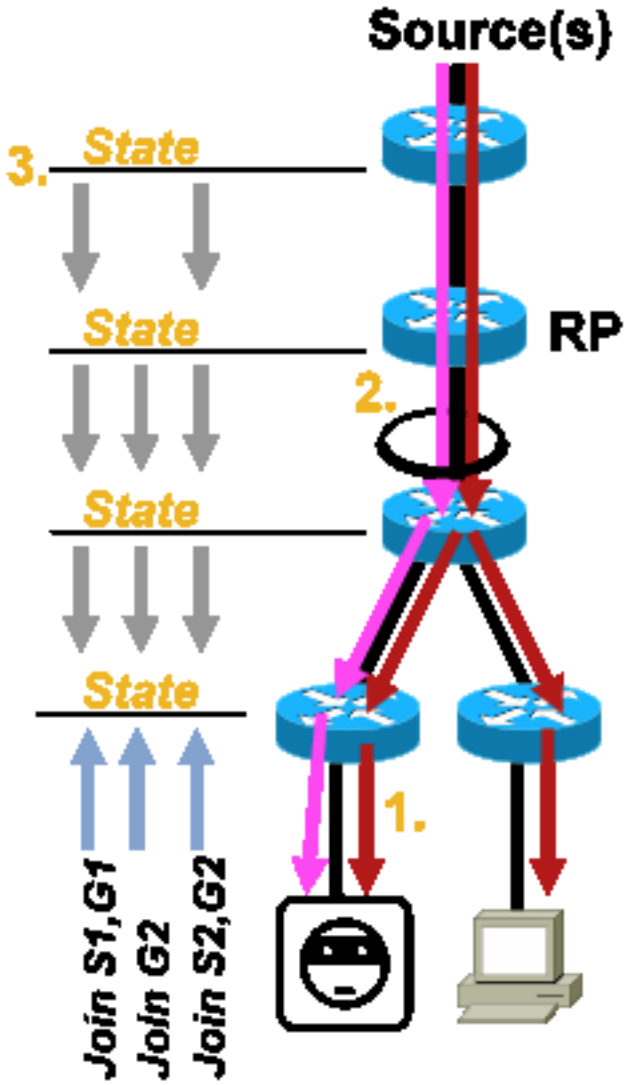

Fig5_Receiver_Explicit_Join

Les attaques des récepteurs peuvent être de trois types :

1. Un récepteur multidiffusion peut tenter de rejoindre un flux pour lequel il n'est pas autorisé et tenter de recevoir du contenu qu'il n'est pas autorisé à recevoir.
2. Un récepteur de multidiffusion peut potentiellement surcharger la bande passante réseau disponible en s'intéressant à de nombreux groupes ou canaux. Ce type d'attaque devient une attaque de bande passante partagée contre d'autres destinataires potentiels de contenu.
3. Un récepteur de multidiffusion peut tenter de lancer une attaque contre des routeurs ou des commutateurs. Un grand nombre de rapports IGMP peuvent être générés, ce qui peut créer une grande quantité d'état d'arborescence de multidiffusion et potentiellement surcharger la capacité du routeur. Ceci peut à son tour entraîner une augmentation des temps de convergence de multidiffusion ou un déni de service sur le routeur.

Vous trouverez dans la section suivante, Sécurité au sein d'un réseau multidiffusion, différentes méthodes permettant de limiter ce type d'attaque.

Sécurité dans un réseau multidiffusion

sécurité des éléments du réseau

La sécurité n'est pas une fonctionnalité ponctuelle, mais une partie intrinsèque de chaque conception de réseau. La sécurité doit donc être prise en compte à chaque point du réseau. Il est primordial que chaque élément du réseau soit correctement sécurisé. Un scénario d'attaque possible, applicable à toute technologie, est un routeur subverti par un intrus. Une fois qu'un intrus a le contrôle d'un routeur, l'attaquant peut exécuter un certain nombre de scénarios d'attaque différents. Chaque élément de réseau doit donc être protégé de manière appropriée contre toute forme d'attaque de base, ainsi que contre des attaques multidiffusion spécifiques.

Contrôle du plan de contrôle (CoPP)

CoPP est l'évolution des listes de contrôle d'accès des routeurs (rACL), disponibles sur la plupart des plates-formes. Le principe est identique : seul le trafic destiné au routeur est réglementé par le protocole CoPP.

La stratégie de service utilise la même syntaxe que toute stratégie de qualité de service, avec policy-maps et class-maps. Par conséquent, il étend la fonctionnalité des rACL (permit/deny) avec des limiteurs de débit pour certains trafics vers le plan de contrôle.

> **Note**: CoPP est activé par défaut sur certaines plates-formes, telles que les commutateurs de la gamme Catalyst 9000, et la protection n'est pas remplacée. Consultez le guide CoPP pour plus d'informations.

Si vous décidez d'ajuster, de modifier ou de créer des listes de contrôle d'accès r ou CoPP dans un réseau actif, veillez à prendre les précautions nécessaires. Étant donné que les deux fonctions peuvent filtrer tout le trafic vers le plan de contrôle, tous les protocoles requis du plan de contrôle et du plan de gestion doivent être explicitement autorisés. La liste des protocoles requis est longue et il peut être facile d'ignorer des protocoles moins évidents tels que le système de contrôle d'accès au contrôleur d'accès aux terminaux (TACACS). Toutes les configurations rACL et CoPP non par défaut doivent toujours être testées dans un environnement de laboratoire avant le déploiement sur les réseaux de production. En outre, les déploiements initiaux doivent commencer par une politique d'autorisation uniquement. Cela permet de valider les résultats inattendus avec les compteurs de résultats ACL.

Dans un environnement de multidiffusion, les protocoles de multidiffusion requis (PIM, MSDP, IGMP, etc.) doivent être autorisés dans rACL ou CoPP pour que la multidiffusion fonctionne correctement. Il est important de se rappeler que le premier paquet dans un flux de multidiffusion provenant de la source dans un scénario PIM-SM est utilisé comme paquet de plan de contrôle, pour aider à créer un état de multidiffusion, jusqu'au plan de contrôle du périphérique. Par conséquent, il est important d'autoriser les groupes de multidiffusion appropriés dans rACL ou CoPP. Étant donné qu'il existe un certain nombre d'exceptions spécifiques à la plate-forme, il est important de consulter la documentation appropriée et de tester toute configuration planifiée avant le déploiement.

Service de transport de paquets local (LPTS)

Sur Cisco IOS XR, le service LPTS (Local Packet Transport Service) sert de régulateur du trafic vers le plan de contrôle du routeur, comme le protocole CoPP sur Cisco IOS. En outre, le trafic de réception, qui inclut le trafic de monodiffusion et de multidiffusion, peut être filtré et limité en débit.

Sécurité spécifique à la multidiffusion

Dans un réseau compatible avec la multidiffusion, chaque élément de réseau doit être sécurisé par des fonctions de sécurité spécifiques à la multidiffusion. Elles sont décrites dans cette section, pour la protection générique des routeurs. Les fonctionnalités qui ne sont pas requises sur chaque routeur, mais uniquement à des emplacements spécifiques du réseau, et les fonctionnalités qui nécessitent une interaction entre les routeurs (telles que l'authentification PIM) sont abordées dans la section suivante.

Limites Mroute

La commande mroute limit limite globalement le nombre de routes de multidiffusion sur un routeur et aide à empêcher les attaques DoS.

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

Figure 6 : Limites Mroute

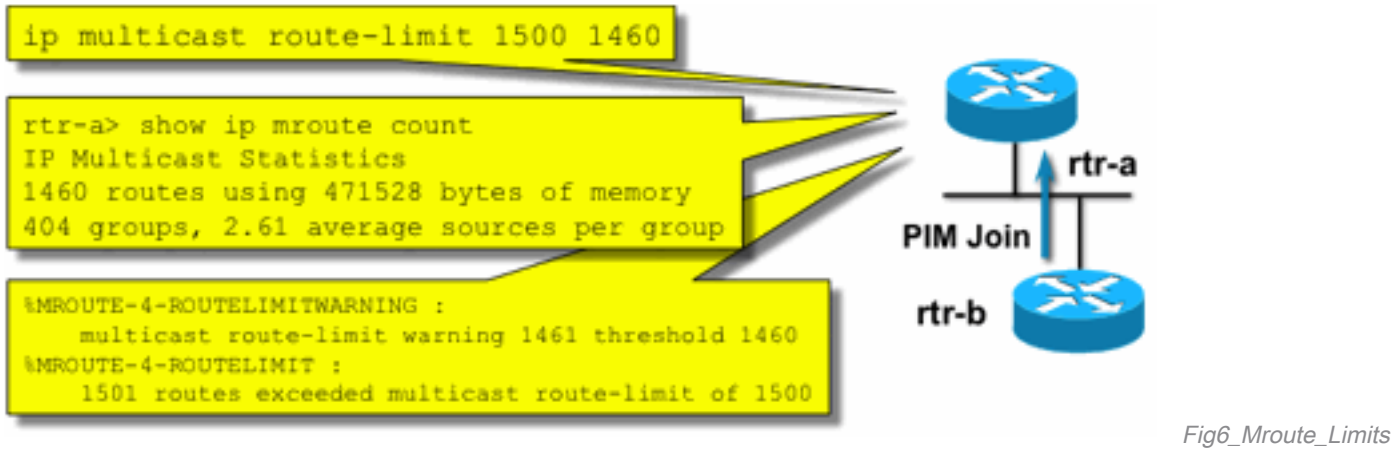

Fig6_Mroute_Limits

Les limites Mroute permettent de définir un seuil sur le nombre de mroutes autorisées dans la table de routage multidiffusion. Si une limite de route de multidiffusion est activée, aucun état de multidiffusion n'est créé au-delà de la limite configurée. Il existe également un seuil d'avertissement. Lorsque le nombre de mroutes dépasse le seuil d'avertissement, des messages d'avertissement syslog sont déclenchés. À la limite mroute, tous les paquets supplémentaires qui déclencheraient l'état sont rejetés.

La commande **ip multicast route-limit** est également disponible par MVRF.

Désactiver l'écoute SAP : no ip sap listen

La commande **sap listen** entraîne la réception par un routeur de messages SAP/SDP (Session Announcement Protocol/Session Description Protocol). SAP/SDP est un protocole hérité qui date des jours du réseau fédérateur de multidiffusion (MBONE). Ces messages indiquent des

informations de répertoire sur le contenu de multidiffusion qui sont disponibles dans le futur ou à l'heure actuelle. Il peut s'agir d'une source de déni de service par rapport aux ressources processeur et mémoire du routeur. Par conséquent, cette fonctionnalité doit être désactivée.

Contrôler l'accès aux informations mrinfo - la commande "ip multicast mrinfo-filter"

La commande mrinfo (disponible sur Cisco IOS et sur certaines versions de Microsoft Windows et Linux) utilise divers messages pour interroger un routeur de multidiffusion afin d'obtenir des informations. La commande de configuration globale **ip multicast mrinfo-filter** peut être utilisée pour limiter l'accès à ces informations à un sous-ensemble de sources, ou le désactiver complètement.

Cet exemple refuse les requêtes provenant de 192.168.1.1, alors que les requêtes sont autorisées à partir de toute autre source :

```
ip multicast mrinfo-filter 51

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

Cet exemple refuse *mrinfo* requêtes de toute source :

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

> **Note**: Comme prévu avec n'importe quelle ACL, un *deny* signifie que le paquet est filtré, tandis qu'un *permit* signifie que le paquet est autorisé.

Si la commande **mrinfo** est utilisée à des fins de diagnostic, il est fortement recommandé de configurer la commande **ip multicast mrinfo-filter** avec une liste de contrôle d'accès appropriée pour autoriser les requêtes uniquement à partir d'un sous-ensemble d'adresses sources. Les informations fournies par la commande *mrinfo* peuvent également être récupérées via SNMP. Des blocs complets de requêtes mrinfo (bloquer toute source à partir des requêtes du périphérique) sont fortement recommandés.

Sécurité du réseau

Dans cette section, différentes façons de sécuriser les paquets de contrôle de multidiffusion et de monodiffusion PIM, ainsi que Auto-RP et BSR, sont décrites.

Désactiver les groupes multidiffusion

Les commandes **ip multicast group-range/ipv6 multicast group range** peuvent être utilisées pour désactiver toutes les opérations pour les groupes refusés par l'ACL :

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

Si des paquets apparaissent pour l'un des groupes refusés par la liste de contrôle d'accès, ils sont

abandonnés dans tous les protocoles de contrôle, y compris PIM, IGMP, MLD et MSDP, et sont également abandonnés dans le plan de données. Par conséquent, aucune entrée de cache IGMP/MLD, aucun état PIM, Multicast Routing Information Base/Multicast Forwarding Information Base (MRIB/MFIB) ne sont jamais créés pour ces plages de groupes et tous les paquets de données sont immédiatement abandonnés.

Ces commandes sont entrées dans la configuration globale du périphérique.

Il est recommandé de déployer cette commande sur tous les routeurs du réseau, quand et où elle est disponible, afin que tout le trafic de multidiffusion provenant de l'extérieur du réseau soit contrôlé. Notez que ces commandes affectent le plan de données et le plan de contrôle. Lorsqu'elle est disponible, cette commande offre une couverture plus étendue que les listes de contrôle d'accès standard et est préférable.

Sécurité PIM

Contrôle de voisin PIM

Un routeur PIM doit recevoir des HELLO PIM pour établir un voisinage PIM. Le voisinage PIM est également à la base de la sélection du routeur désigné (DR) et du basculement du DR, ainsi que des messages PIM Join/Prune/Assert envoyés/reçus.

Figure 7 : Contrôle de voisin PIM

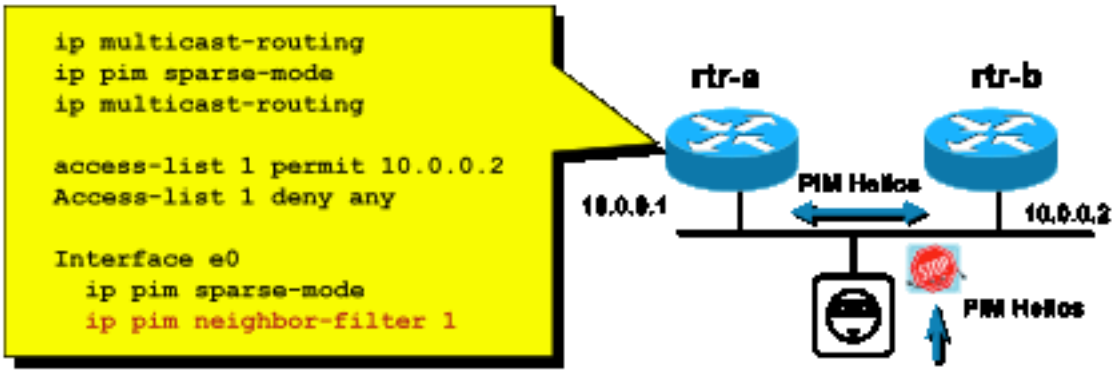

Fig7_PIM_neighbor_control

Pour empêcher les voisins indésirables, utilisez la **ip pim neighbor-filter** Cette commande filtre tous les paquets PIM voisins non autorisés, ce qui inclut les paquets Hello, Join/Prune et BSR. Les hôtes sur le segment peuvent potentiellement usurper l'adresse IP source pour prétendre être le voisin PIM. Des mécanismes de sécurité de couche 2 (à savoir la protection de la source IP) sont nécessaires pour empêcher les adresses source d'une tentative d'usurpation sur un segment ou pour utiliser une liste de contrôle d'accès VLAN dans le commutateur d'accès afin d'empêcher les paquets PIM des hôtes. Le mot clé « log-input » peut être utilisé dans les listes de contrôle d'accès pour consigner les paquets qui correspondent à l'ACE.

Le paquet PIM Join/Prune est envoyé à un voisin PIM pour ajouter ou supprimer ce voisin d'un chemin particulier (S, G) ou (*, G). Les paquets de multidiffusion PIM sont des paquets de multidiffusion locale de liaison envoyés avec une durée de vie (TTL) = 1. Tous ces paquets sont

multidiffusés à l'adresse connue de tous les routeurs PIM : 224.0.0.13 . Cela signifie que toutes ces attaques doivent provenir du même sous-réseau que le routeur attaqué. Les attaques peuvent inclure de faux paquets Hello, Join/Prune et Assert.

> **Note**: Une augmentation ou un ajustement artificiel de la valeur TTL dans des paquets de multidiffusion PIM à une valeur supérieure à 1 ne crée pas de problèmes. L'adresse All-PIM-Routers est toujours reçue et traitée localement sur un routeur. Il n'est jamais directement transféré par des routeurs normaux et légitimes.

Pour protéger le RP contre un flux potentiel de messages de registre PIM-SM, le DR doit limiter le débit de ces messages. Utilisez la commande **ip pim register-rate-limit** :

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

Figure 8 : Contrôle de tunnel du registre PIM-SM

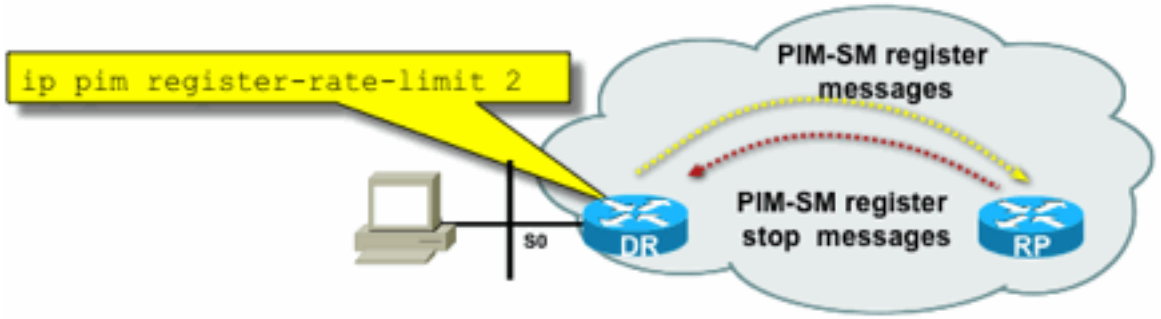

Fig8_PIMSM_Reg Tunnel

Les paquets de monodiffusion PIM peuvent être utilisés pour attaquer le RP. Par conséquent, le RP peut être protégé par des ACL d'infrastructure contre de telles attaques. Rappelez-vous que les expéditeurs et les récepteurs de multidiffusion n'ont jamais besoin d'envoyer des paquets PIM, de sorte que le protocole PIM (protocole IP 103) peut généralement être filtré à la périphérie de l'abonné.

Contrôle Auto-RP - Filtre d'annonce RP

La commande **ip pim rp-announce filter** est une mesure de sécurité supplémentaire qui peut être configurée avec Auto-RP si possible :

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

Il peut être configuré sur l'agent de mappage pour contrôler quels routeurs sont acceptés comme RP candidats pour quelles plages de groupes / mode groupe.

Figure 9 : Auto-RP - Filtre d'annonce RP

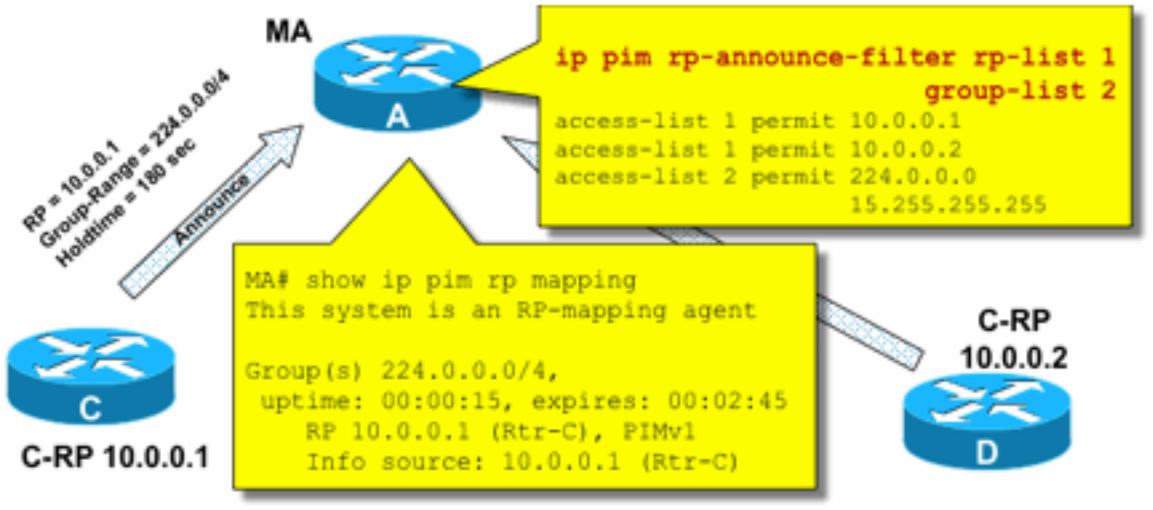

Fig9_AutoRP_RP_Announce

Contrôle Auto-RP - Contraindre les messages Auto-RP

Utilisez la commande multicast border pour contraindre les paquets AutoRP, RP-announce (224.0.1.39) ou RP-discover (224.0.1.40) à un domaine PIM particulier :

```
ip multicast boundary
```

Figure 10 : Commande Multicast Boundary

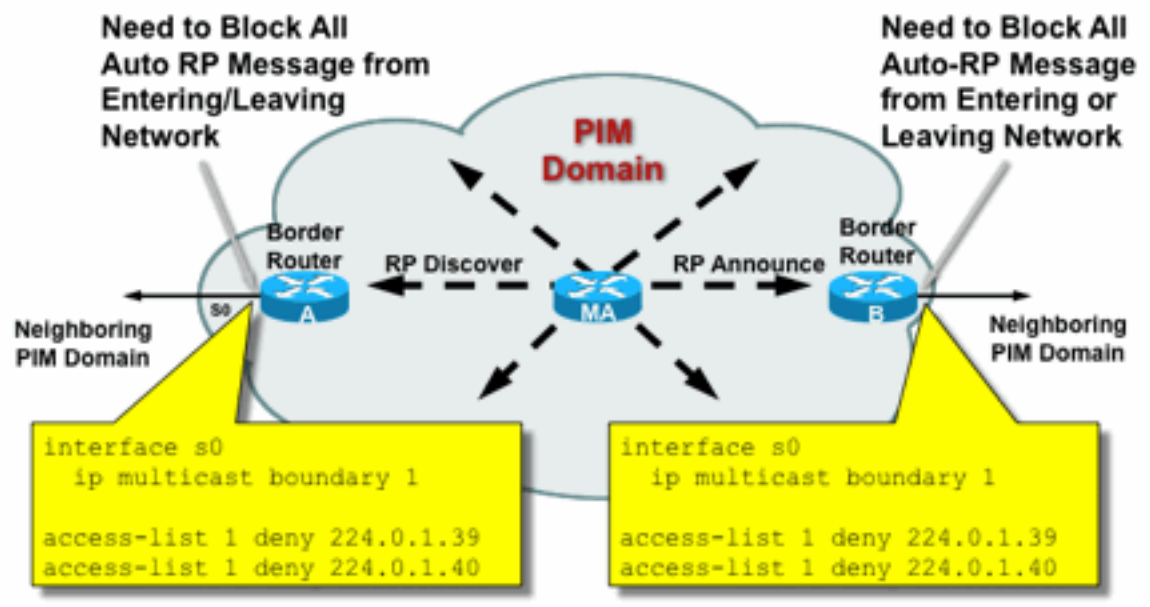

Fig10_Mcast_Boundary

Contrôle BSR - Contraindre les messages BSR

Utilisez **ip pim bsr-border** pour filtrer les messages BSR à la frontière d'un domaine PIM. Aucune liste de contrôle d'accès n'est nécessaire car les messages BSR sont transférés saut par saut avec la multidiffusion link-local.

Figure 11 : Bordure BSR

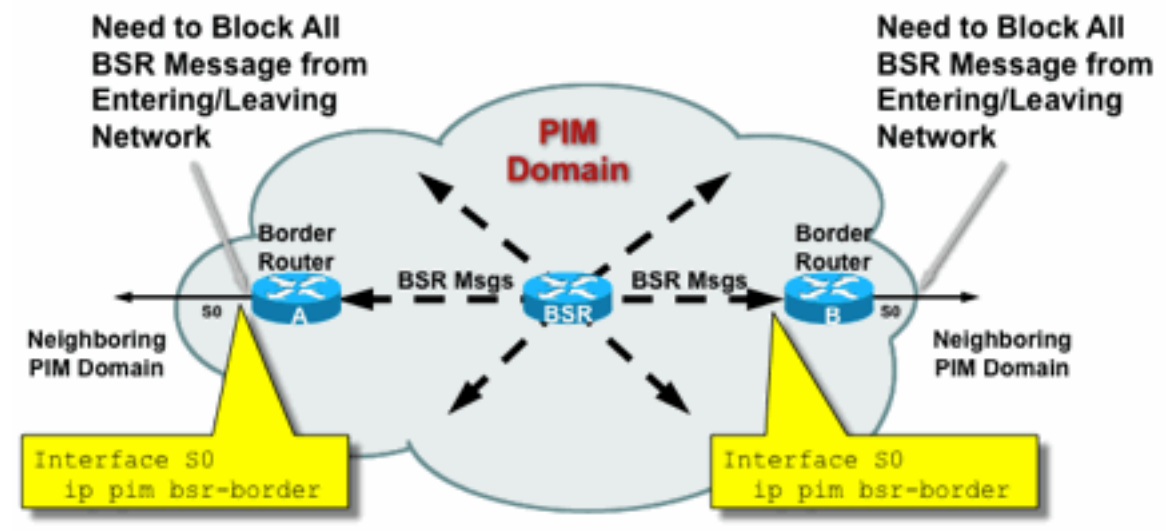

Fig11_BSR_Router

Filtres liés à RP / PIM-SM

Dans le cadre de cette dernière section, les filtres contre les paquets de plan de contrôle PIM-SP et RP ainsi que les messages Auto-RP, BSR et MSDP sont abordés.

Filtres Auto-RP

La Figure 12 présente un exemple de filtres Auto-RP associés à des étendues d'adresses. Deux manières différentes de lier une région sont présentées. Les deux listes de contrôle d'accès sont équivalentes du point de vue du protocole Auto-RP.

Figure 12 : Filtres/étendues Auto-RP

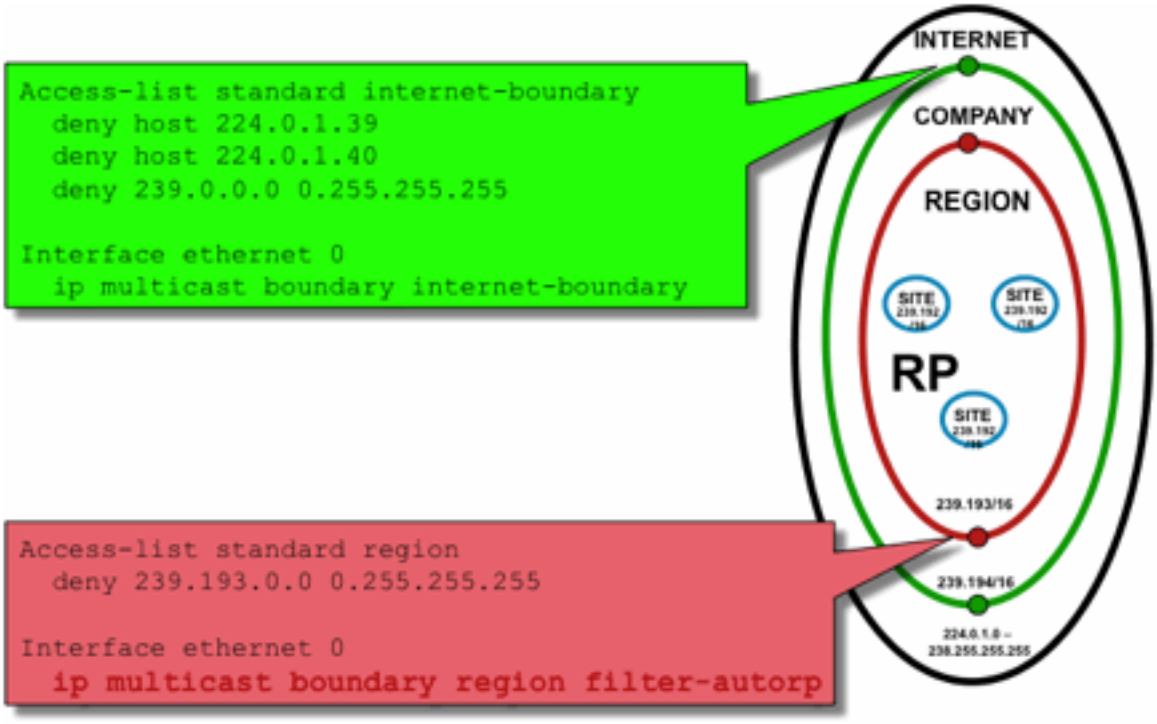

Fig12_AutoRP_Filtering_Scoping

L'idée des filtres de limite d'interface pour Auto-RP est de s'assurer que les annonces auto-RP atteignent seulement les régions qu'elles prennent en charge. Des étendues régionales, d'entreprise et à l'échelle d'Internet sont définies, et dans chaque cas, il y a des RP et des annonces Auto-RP dans chaque étendue. Les administrateurs veulent seulement que les RP régionaux soient connus des routeurs régionaux, que les RP d'entreprise soient connus des routeurs régionaux et d'entreprise et que tous les RP Internet soient disponibles dans le monde entier. D'autres niveaux de portée sont possibles.

Comme le montre l'image, il existe deux façons fondamentalement différentes de filtrer les paquets Auto-RP : La frontière Internet appelle explicitement les groupes de contrôle auto-RP (224.0.1.39 et 224.0.1.40), ce qui entraîne des filtres contre tous les paquets Auto-RP. Cette méthode peut être utilisée à la périphérie d'un domaine administratif, où aucun paquet Auto-RP n'est transmis. La limite de région utilise le mot clé filter-auto-rp pour provoquer un examen des annonces rp-to-group-range dans les paquets Auto-RP. Lorsqu'une annonce est explicitement refusée par la liste de contrôle d'accès, elle est supprimée du paquet Auto-RP avant que le paquet ne soit transféré. Dans l'exemple, cela permet de connaître les RP de l'entreprise dans les régions, tandis que les RP de la région sont filtrés à la frontière entre la région et le reste de l'entreprise.

Filtres interdomaines et MSDP

Dans cet exemple, ISP1 agit en tant que fournisseur de transit PIM-SM. Ils prennent uniquement en charge l'appairage MSDP avec les voisins et acceptent uniquement (S, G), mais aucun trafic (*, G) sur les routeurs périphériques.

Dans le domaine inter-domaine (généralement entre systèmes autonomes), deux mesures de sécurité de base doivent être prises :

1. Sécurisez le plan de données, via la commande **multicast border**. Cela garantit que le trafic de multidiffusion est uniquement accepté pour les groupes définis (et les sources potentielles).
2. Sécurisez le trafic du plan de contrôle interdomaine (MSDP). Il s'agit d'un certain nombre de mesures de sécurité distinctes : Contrôle du contenu MSDP, limitation de l'état et authentification des voisins.

La Figure 13 présente un exemple de configuration d'un filtre d'interface sur l'un des routeurs périphériques du routeur ISP1.

Pour sécuriser le plan de données à la limite du domaine, interdisez (*,G) les jonctions par filtres contre les adresses « hôte 0.0.0.0 » et étendues administrativement via la commande **multicast border** :

Figure 13 : Filtre interdomaine (*,G)

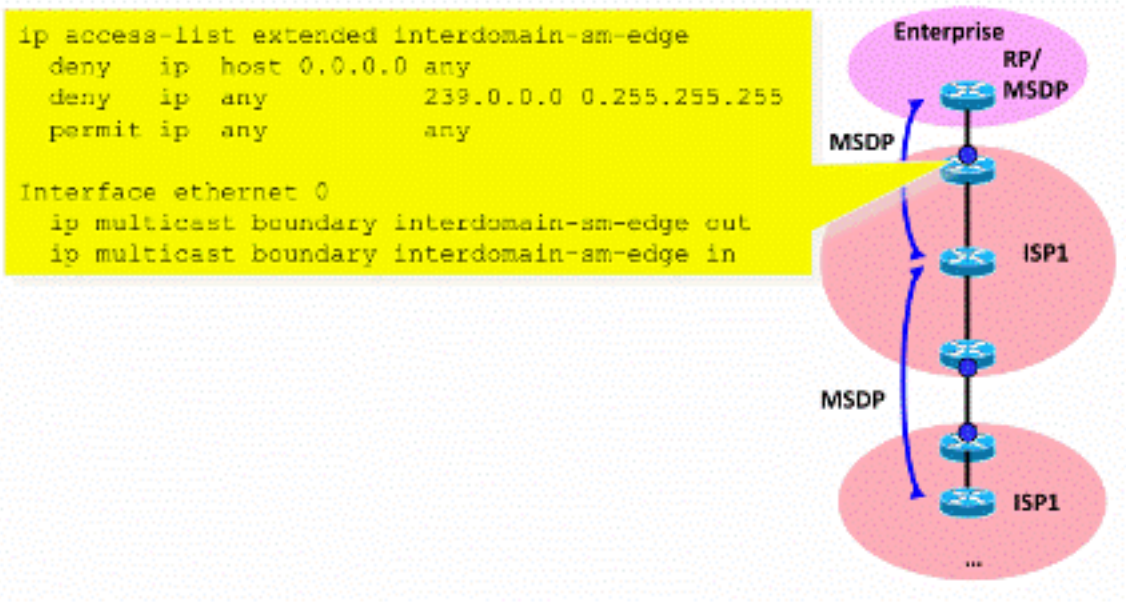

Fig13_Interdomain_Filter

Pour sécuriser le plan de contrôle, renforcez MSDP via trois mesures de sécurité de base :

1) Filtres SA MSDP

Il est recommandé de filtrer le contenu des messages MSDP via les filtres SA MSDP. L'idée principale de ce filtre est d'éviter la propagation de l'état de multidiffusion pour les applications et les groupes qui ne sont pas des applications Internet et qui n'ont pas besoin d'être transférés au-delà du domaine source. Idéalement, du point de vue de la sécurité, les filtres n'autorisent que les groupes connus (et potentiellement les expéditeurs) et refusent tous les expéditeurs et/ou groupes inconnus.

Il est généralement impossible de répertorier explicitement tous les expéditeurs et/ou groupes autorisés. il est recommandé d'utiliser le filtre de configuration par défaut pour les domaines PIM-SM avec un RP unique pour chaque groupe (pas de groupe de maillage 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 !
```

Il est recommandé de filtrer le plus strictement possible, et dans les deux sens, en entrée et en sortie.

Pour plus d'informations sur les recommandations de filtre SA MSDP, consultez la page : https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) Limitation de l'état MSDP

Lorsque MSDP est activé entre plusieurs systèmes autonomes (AS), il est recommandé de limiter la quantité d'état qui est construite dans le routeur en raison des messages « Source-Active » (SA) reçus des voisins. Vous pouvez utiliser la commande **ip msdp sa-limit** :

ip msdp sa-limit <peer> <limit>

Figure 14 : Plan de contrôle MSDP

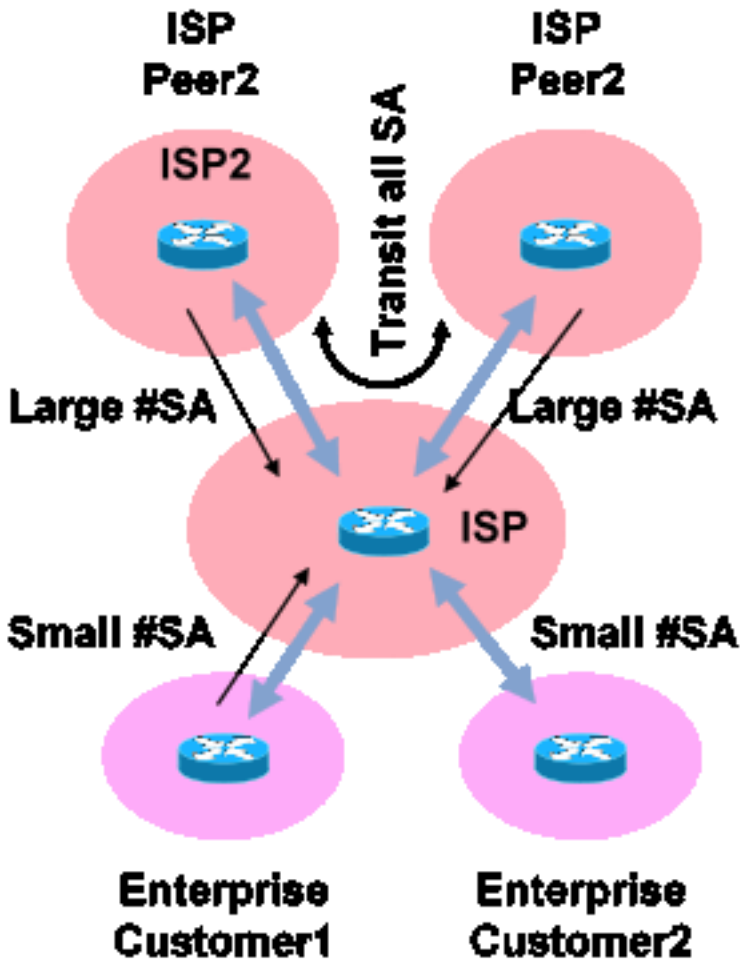

Fig14_MSDP_ControlPlane

Avec la commande **ip msdp sa-limit** vous pouvez limiter le nombre d'états SA créés en raison des messages SA acceptés d'un homologue MSDP. Voici quelques recommandations générales simples :

- Petite limite de stub-neighbor
- Limite importante du voisin de transit (par exemple #SAs maximum dans Internet)
- Transit ISP : configurez le #SAs maximum pris en charge par votre plate-forme

3) Authentification de voisin MD5 MSDP

Il est recommandé d'utiliser l'authentification par mot de passe MD5 (Message-Digest Algorithm) sur les homologues MSDP. Cette option utilise l'option de signature TCP MD5, équivalente à l'utilisation décrite dans RFC 6691 pour sécuriser BGP.

Figure 15 : Authentification de voisin MD5 MSDP

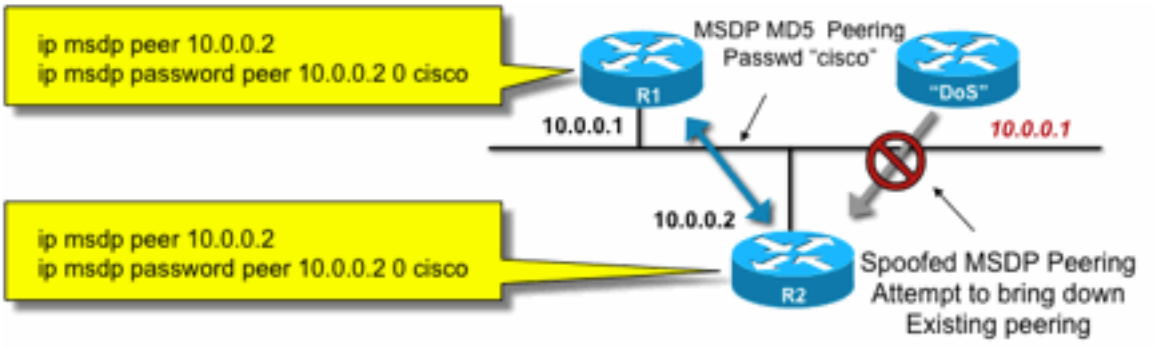

Fig15_MSDP_MD5Auth

Ces trois recommandations de sécurité MSDP poursuivent des objectifs différents :

- L'authentification de voisin (avec MD5) garantit que seuls les homologues MSDP approuvés peuvent envoyer des messages.
- Les filtres SA garantissent que même un homologue MSDP approuvé peut uniquement envoyer des annonces SA qui sont conformes à la stratégie source/groupe prédéfinie.
- La limite SA garantit également que même avec des annonces légitimes (S, G) provenant d'homologues légitimes, la mémoire disponible ne peut pas être épuisée.

Problèmes expéditeur/source

De nombreux problèmes de sécurité de multidiffusion qui proviennent de l'expéditeur peuvent être atténués par des mécanismes de sécurité de monodiffusion appropriés. Un certain nombre de mécanismes de sécurité de monodiffusion sont recommandés ici :

- **Protection contre l'usurpation d'adresse source** (Unicast Reverse Path Forwarding, uRPF ou ACL et IP source guard pour la couche d'accès)
- **ACL d'infrastructure** (deny ip any (to) <espace d'adressage principal>)

De telles mesures peuvent être utilisées pour bloquer les attaques dirigées sur le coeur. Cela permettrait, par exemple, de résoudre des problèmes tels que des attaques qui utilisent des paquets de monodiffusion PIM vers le RP, qui est « interne » au réseau et serait donc protégé par la liste de contrôle d'accès d'infrastructure.

Contrôle d'accès basé sur le filtre de paquets - Sources de contrôle

Dans l'exemple de la Figure 16, le filtre est configuré sur l'interface LAN (E0) du routeur de multidiffusion de premier saut (Designated Router). Le filtre est défini par une liste de contrôle d'accès étendue appelée « source ». Cette liste de contrôle d'accès est appliquée à l'interface orientée source du routeur désigné connecté au réseau local source. En fait, en raison de la nature du trafic de multidiffusion, il peut être nécessaire de configurer un filtre similaire sur toutes les interfaces orientées LAN sur lesquelles les sources peuvent devenir actives. Étant donné qu'il n'est pas possible dans tous les cas de savoir exactement où l'activité source se produit, il est recommandé d'appliquer de tels filtres à tous les points d'entrée du réseau.

Figure 16 : Sources de contrôle

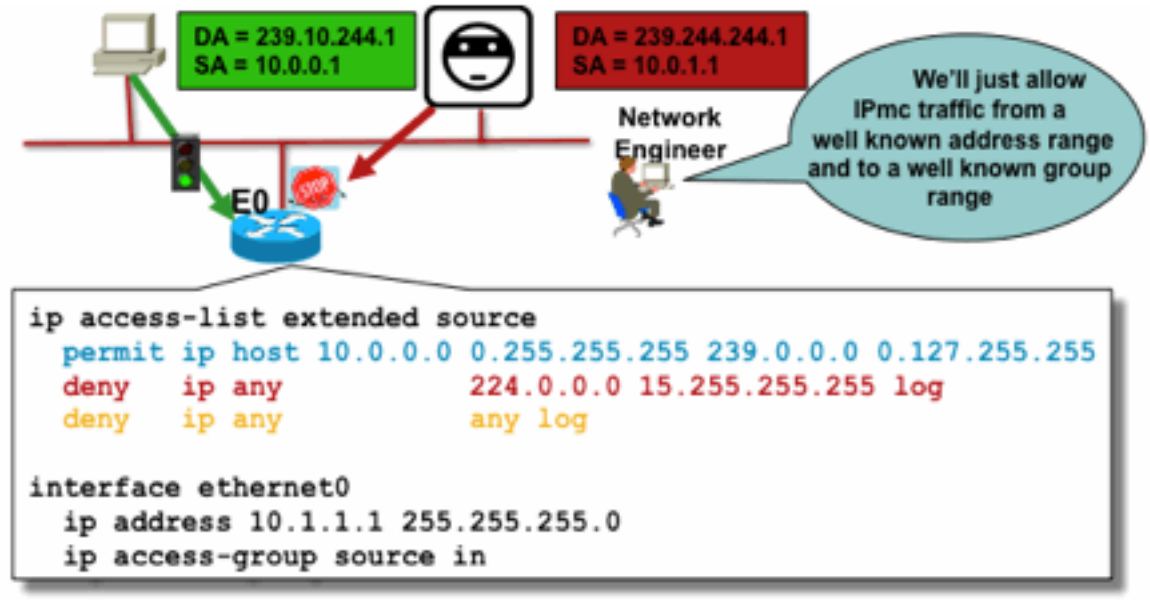

Fig16_Contrôle_Sources

L'objectif de ce filtre est d'empêcher le trafic d'une source ou plage spécifique d'adresses source vers un groupe ou une plage spécifique d'adresses de groupe. Ce filtre agit avant que PIM ne crée des mroutes et aide à limiter l'état.

Il s'agit d'une liste de contrôle d'accès standard. Ceci est mis en oeuvre sur des ASIC sur des plates-formes haut de gamme, et aucune pénalité de performance n'est encourue. Les listes de contrôle d'accès du plan de données sont recommandées et préférées au plan de contrôle pour les sources directement connectées, car elles minimisent l'impact du trafic indésirable sur le plan de contrôle. Il est également très efficace de limiter la destination (adresses de groupe de multidiffusion IP) vers laquelle les paquets peuvent être envoyés. Comme il s'agit d'une commande de routeur, elle ne peut pas surmonter une adresse IP source usurpée (voir la partie précédente de cette section). Par conséquent, il est recommandé de fournir des mécanismes de couche 2 (L2) supplémentaires ou une politique cohérente pour tous les périphériques qui peuvent se connecter à un réseau local/réseau local virtuel (LAN/VLAN) particulier.

> **Note**: Le mot clé « log » dans une liste de contrôle d'accès est très utile pour comprendre les occurrences d'une entrée spécifique ; toutefois, cela consomme des ressources processeur et doit être géré avec précaution. En outre, sur les plates-formes matérielles, les messages de journal des listes de contrôle d'accès sont produits par un processeur, et l'impact sur le processeur doit donc être pris en compte.

Contrôle de source PIM-SM

L'un des avantages réels de l'architecture ASM / PIM-SM du point de vue de la sécurité est le fait que le point de rendez-vous donne un point de contrôle unique pour toutes les sources du réseau pour n'importe quelle plage de groupe. Cela peut être exploité avec un périphérique appelé le filtre accept-register. La commande de ce filtre est la suivante :

ip pim accept-register / ipv6 pim accept-register

Figure 17 : Contrôle de source PIM-SM

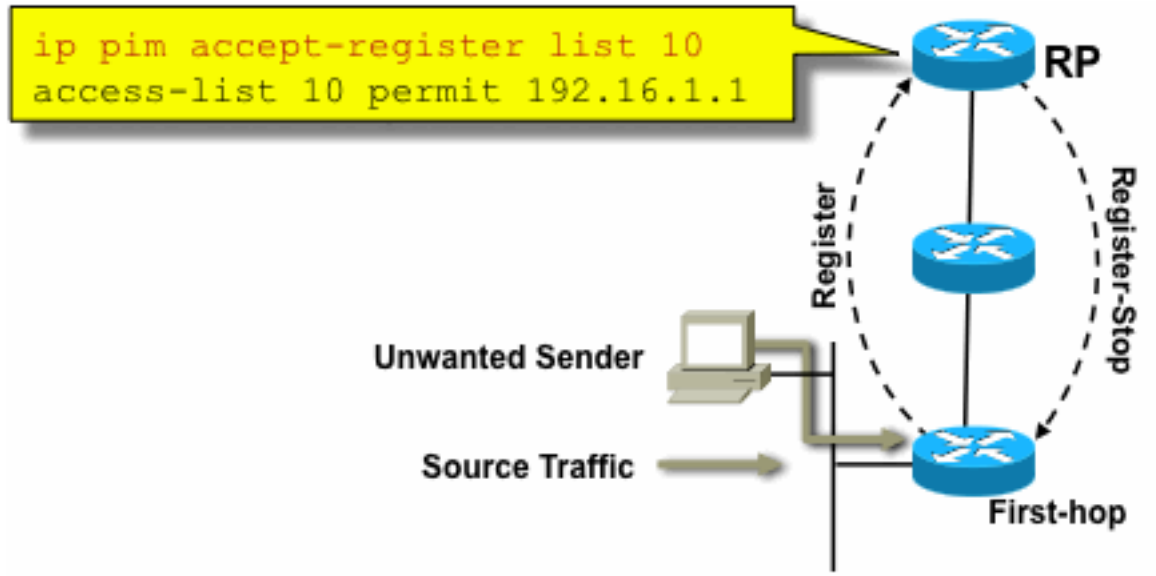

Fig17_PIMSM_Control

Dans un réseau PIM-SM, une source de trafic indésirable peut être contrôlée avec cette commande. Lorsque le trafic source atteint le routeur de premier saut, le routeur de premier saut (DR) crée un état (S, G) et envoie un message PIM Source Register au RP. Si la source n'est pas répertoriée dans la liste de filtres accept-register (configurée sur le RP), le RP rejette le Register et renvoie un message Register-Stop immédiat au DR.

Dans l'exemple illustré, une liste de contrôle d'accès simple a été appliquée au RP, qui filtre uniquement l'adresse source. Il est également possible de filtrer la source ET le groupe à l'aide d'une liste de contrôle d'accès étendue sur le RP.

Il y a des inconvénients avec les filtres source parce qu'avec la commande **pim accept-register** sur le RP, l'état PIM-SM (S, G) est toujours créé sur le routeur de premier saut de la source. Cela peut entraîner un trafic au niveau des récepteurs locaux à la source et situés entre la source et le RP. En outre, la commande **pim accept-register** fonctionne sur le plan de contrôle du RP. Cela pourrait être utilisé pour surcharger le RP avec de faux messages de registre, et peut-être causer une condition de DoS.

Il est recommandé d'appliquer la commande pim accept-register sur le RP en plus d'autres méthodes, telles que l'application de listes de contrôle d'accès de plan de données simples sur tous les DR, sur tous les points d'entrée dans le réseau. Alors que les listes de contrôle d'accès d'entrée sur le DR seraient suffisantes dans un réseau parfaitement configuré et exploité, il est recommandé de configurer la commande **pim accept-register** sur le RP en tant que mécanisme de sécurité secondaire en cas de mauvaise configuration sur les routeurs de périphérie. Les mécanismes de sécurité multicouche ayant le même objectif sont appelés « défense en profondeur » et constituent un principe de conception courant en matière de sécurité.

Problèmes de récepteur - Contrôle IGMP/MLD

La plupart des problèmes de récepteur relèvent du domaine des interactions de protocole de récepteur IGMP/MLD.

Figure 18 : Contrôle IGMP

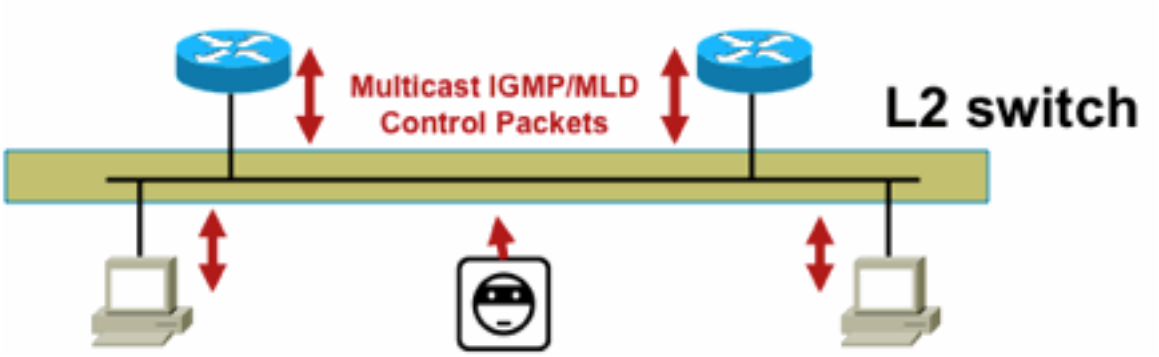

Fig18_Contrôle_IGMP

Lorsque des paquets IGMP ou MLD sont filtrés, n'oubliez pas ces points :

- IPv4: IGMP est un type de protocole IPv4 (protocole IPv4 2)
- IPv6 : MLD est transporté dans des paquets de type protocole ICMPv6

Le processus IGMP est activé par défaut dès que la multidiffusion IP est activée. Les paquets IGMP transportent également ces protocoles, et par conséquent tous ces protocoles sont activés chaque fois que la multidiffusion est activée :

- PIMv1 : PIMv1 était la première version de PIM et est toujours activé dans Cisco IOS à des fins de migration. Les déploiements actuels utilisent tous PIMv2.
- Mrinfo - Mrinfo est une commande Unix héritée par Cisco IOS pour afficher les voisins de multidiffusion. Cisco recommande l'utilisation de SNMP au lieu de la commande mrinfo.
- DVMRP : le protocole DVMRP est un protocole à vecteur de distance hérité en mode dense dont les caractéristiques d'évolutivité sont très limitées. La prise en charge de Cisco IOS pour DVMRP est abandonnée ou déjà déconseillée.
- Mtrace : Mtrace est l'équivalent multidiffusion de « traceroute » monodiffusion et constitue un outil utile

Pour plus d'informations, voir Numéros de type IGMP (Internet Group Management Protocol) de l'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
```

Les paquets IGMP monodiffusion (pour IGMP/UDLR) peuvent être filtrés, car il s'agit très probablement de paquets d'attaque et de paquets de protocole IGMP non valides. Les paquets IGMP monodiffusion sont pris en charge par Cisco IOS pour les liaisons unidirectionnelles et d'autres conditions d'exception.

Les paquets de requête IGMP/MLD falsifiés peuvent entraîner une version d'IGMP inférieure à celle attendue.

En particulier, les hôtes n'envoient idéalement jamais de requêtes IGMP car une requête envoyée avec une version IGMP inférieure peut faire en sorte que tous les hôtes qui reçoivent cette requête reviennent à la version inférieure. En présence d'hôtes IGMPv3/SSM, cela peut « attaquer » les flux SSM. Dans le cas d'IGMPv2, cela peut entraîner des latences de sortie plus longues.

Si un LAN non redondant avec un seul demandeur IGMP est présent, le routeur doit abandonner les requêtes IGMP reçues.

S'il existe un LAN passif redondant/commun, un commutateur capable de surveiller IGMP est requis. Deux fonctionnalités spécifiques peuvent vous aider dans ce cas :

- Protection du routeur
- IGMP version minimale, commande

Protection du routeur

Tout port de commutateur peut devenir un port de routeur multidiffusion si le commutateur reçoit un paquet de contrôle de routeur multidiffusion (requête générale IGMP, PIM Hello ou CGMP Hello) sur ce port. Lorsqu'un port de commutateur devient un port de routeur de multidiffusion, tout le trafic de multidiffusion est envoyé à ce port. Cela peut être évité avec la « protection du routeur ». La fonction Router Guard ne nécessite pas l'activation de la surveillance IGMP.

La fonction Router Guard permet de désigner un port hôte de multidiffusion comme port hôte spécifié. Le port ne peut pas devenir un port de routeur, même si des paquets de contrôle de routeur de multidiffusion sont reçus.

Ces types de paquets sont ignorés s'ils sont reçus sur un port sur lequel Router Guard est activé :

- Messages de requête IGMP
- Messages IPv4 PIMv2
- Messages PIM IGMP (PIMv1)
- Messages IGMP DVMRP
- Messages RGMP (Router-port Group Management Protocol)
- Messages CGMP (Cisco Group Management Protocol)

Lorsque ces paquets sont éliminés, les statistiques sont mises à jour, ce qui indique que les paquets sont abandonnés en raison de la protection du routeur.

Version IGMP minimale

Il est possible de configurer la version minimale des hôtes IGMP autorisés. Par exemple, vous pouvez interdire tous les hôtes IGMPv1 ou tous les hôtes IGMPv1 et IGMPv2. Ce filtre s'applique uniquement aux rapports d'appartenance.

Si les hôtes sont reliés à un LAN « passif » commun (par exemple, un commutateur qui ne prend pas en charge la surveillance IGMP, ou qui n'est pas configuré pour cela), il n'y a également rien qu'un routeur puisse faire à propos de telles fausses requêtes, à part ignorer les rapports d'appartenance « ancienne version » qui sont ensuite déclenchés, et ne pas se replier.

Comme les requêtes IGMP doivent être visibles par tous les hôtes, il n'est pas possible d'utiliser un mécanisme d'authentification de message par hachage (HMAC) avec une clé pré-partagée,

telle que la clé statique IPSec, pour authentifier les requêtes IGMP à partir de « routeurs valides ». Si deux routeurs ou plus sont reliés à un segment LAN commun, une sélection de demandeur IGMP est requise. Dans ce cas, le seul filtre qui pourrait être utilisé est un filtre de groupe d'accès IP basé sur l'adresse IP source de l'autre routeur IGMP qui envoie des requêtes.

Les paquets IGMP de multidiffusion « normaux » doivent être autorisés.

Ce filtre peut être utilisé sur les ports de réception pour autoriser uniquement les paquets IGMP « corrects » et pour filtrer les paquets « défectueux » connus :

```
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
```

> **Note**: Ce type de filtre IGMP peut être utilisé dans les ACL de réception ou CoPP. Dans les deux applications, il doit être associé à des filtres pour d'autres trafics traités, tels que les protocoles de routage et de plan de gestion.

Figure 19 : Contrôle d'accès côté hôte côté récepteur

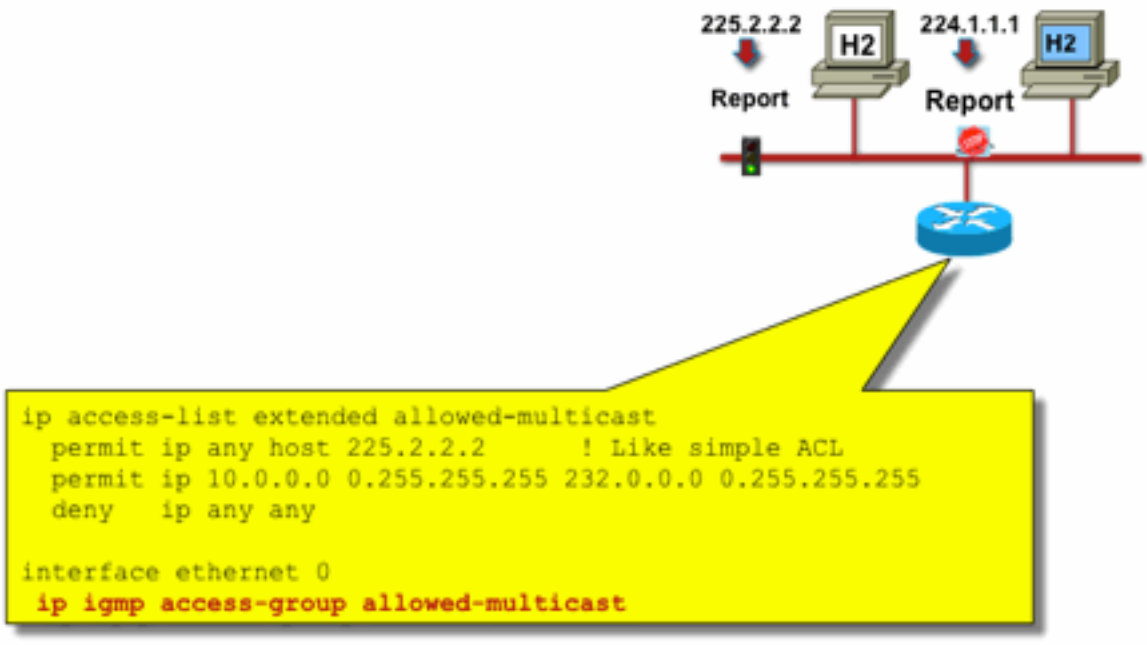

Fig19_Host_Receiver_Access

Pour filtrer le trafic vers un récepteur, ne filtrez pas le trafic du plan de données, mais plutôt le

protocole IGMP du plan de contrôle. Étant donné que le protocole IGMP est une condition préalable nécessaire pour recevoir le trafic de multidiffusion, aucun filtre de plan de données n'est requis.

En particulier, vous pouvez limiter les flux de multidiffusion que les récepteurs peuvent rejoindre (reliés à l'interface sur laquelle la commande est configurée). Dans ce cas, utilisez la commande **ip igmp access-group / ipv6 mld access-group** :

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

Pour les groupes ASM, cette commande filtre uniquement en fonction de l'adresse de destination. L'adresse IP source de la liste de contrôle d'accès est alors ignorée. Pour les groupes SSM qui utilisent IGMPv3 / MLDv2, il filtre les adresses IP source et de destination.

Cet exemple filtre un groupe donné pour tous les haut-parleurs 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
```

Cet exemple filtre des haut-parleurs IGMP spécifiques (donc des récepteurs de multidiffusion spécifiques) pour un groupe donné :

```
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
```

Note: Pour les groupes ASM, la source est ignorée.

Contrôle D'Admission

Le contrôle d'accès fournit une réponse binaire, oui ou non pour certains flux, indépendamment de l'état du réseau. En revanche, le contrôle d'admission limite le nombre de ressources qu'un expéditeur/destinataire peut utiliser, en supposant qu'il a réussi les mécanismes de contrôle d'accès. Divers périphériques sont disponibles pour faciliter le contrôle d'admission dans un environnement de multidiffusion.

Limites IGMP globales et par interface

Au niveau du routeur le plus proche des récepteurs de multidiffusion intéressés, il est possible de limiter le nombre de groupes IGMP joints à la fois globalement et par interface. Vous pouvez utiliser les commandes **ip igmp limit/ipv6 mld limit** :

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

Il est recommandé de toujours configurer cette limite par interface et globalement. Dans chaque cas, la limite fait référence au nombre d'entrées dans le cache IGMP.

Les deux exemples suivants montrent comment cette commande peut être utilisée pour limiter le nombre de groupes à la périphérie d'un réseau haut débit résidentiel.

Exemple 1 : limiter les groupes reçus aux annonces SDR plus un canal reçu

Le répertoire de session (SDR) sert de guide de canal à certains récepteurs de multidiffusion. Consultez RFC 2327 pour plus de détails.

Une exigence courante consiste à limiter les récepteurs à recevoir le groupe SD plus un canal. Cet exemple de configuration peut être utilisé :

```
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 liste d'accès dans cet exemple spécifie uniquement le guide de canal ; la commande globale **ip igmp limit** limite chaque source IGMP à un seul (1) canal, mais n'inclut pas le guide de canal, qui peut toujours être reçu. La commande interface remplace la commande globale et permet la réception de deux (2) canaux, en plus du guide de canaux, sur cette interface.

Exemple 2 : contrôle d'admission sur une liaison d'agrégation-DSLAM

Cette commande peut également être utilisée pour fournir une forme de contrôle d'admission de bande passante. Par exemple, s'il était nécessaire de distribuer 300 canaux SDTV, qui sont de 4 Mbits/s chacun, et qu'il y a une liaison de 1 Gbits/s vers le multiplexeur d'accès de ligne d'abonné numérique (DSLAM), vous pouvez prendre une décision de politique pour limiter la bande passante TV à 500 Mbits/s et laisser le reste pour Internet et d'autres utilisations. Dans ce cas, vous pouvez limiter les états IGMP à 500 Mbits/s/4 Mbits/s = 125 états IGMP.

Cette configuration peut être utilisée dans ce cas :

Figure 20 : Utilisation des limites IGMP par interface ; Contrôle d’admission sur liaison Agg-DSLAM

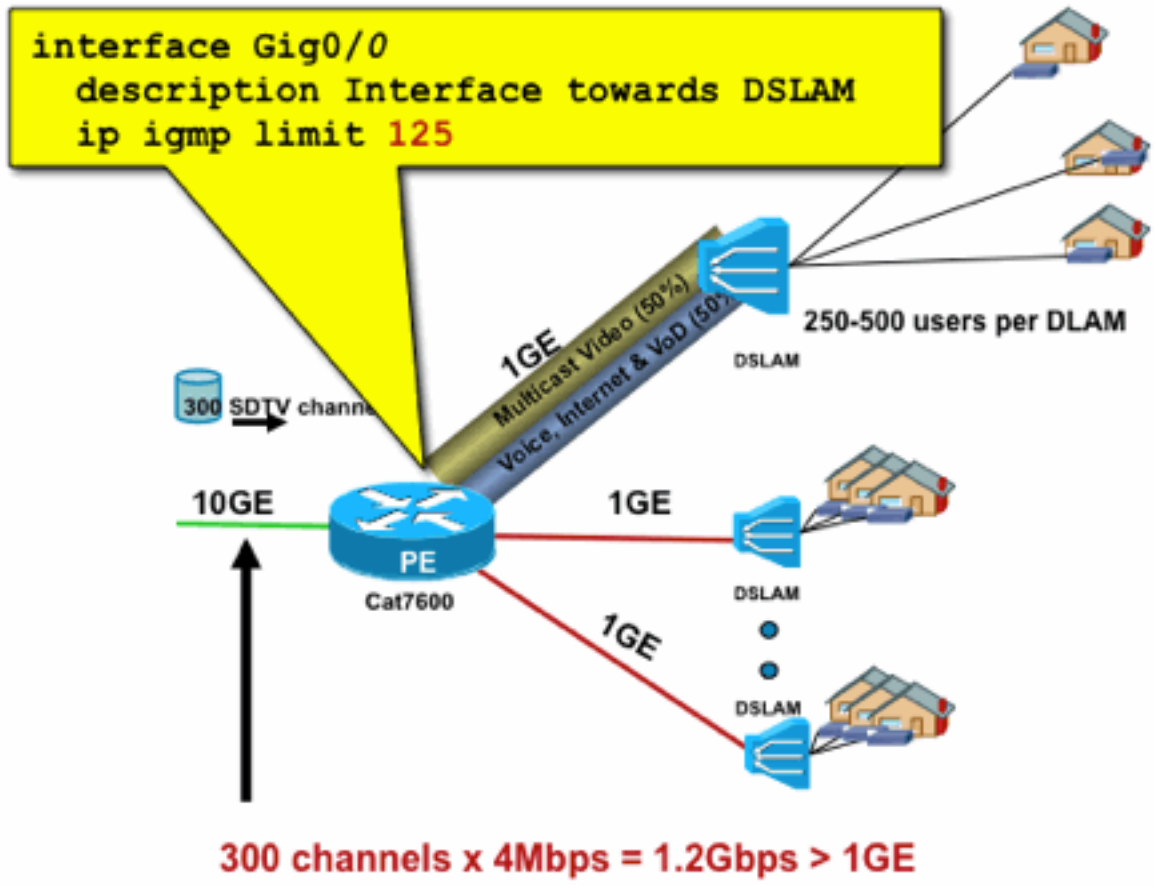

Fig20_PerInterface_IGMP

Limites de mroute par interface

L'activation des limites d'état mroute par interface est une forme plus générique de contrôle d'admission. Il limite non seulement l'état IGMP et PIM sur une interface sortante, mais fournit également un moyen de limiter l'état sur les interfaces entrantes.

Utilisez la commande **ip multicast limit** :

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

L'état peut être limité séparément sur les interfaces d'entrée et de sortie. L'état source connecté directement peut également être limité par l'utilisation du mot clé « connected ». Des exemples illustrent l'utilisation de cette commande :

Exemple 1 : contrôle d'admission en sortie sur une liaison Agg-DSLAM

Dans cet exemple, il y a 300 chaînes TV SD. Supposons que chaque canal SD nécessite 4 Mbits/s, avec un total ne dépassant pas 500 Mbits/s. Enfin, supposez également que des bundles Basic, Extended et Premium sont nécessaires. Exemple d'allocation de bande passante :

- 60 % / 300 Mbit/s de base
- 20 % / 100 Mbit/s étendu
- Premium 20 % / 100 Mbit/s

Ensuite, utilisez 4 Mbits/s par canal et limitez la liaison ascendante DSLAM à :

- 75 états de base
- 25 états étendus
- Premium 25 états

Configurez la limite sur l'interface sortante qui fait face au DSLAM à partir du PEAgg :

Figure 21 : Utilisation des limites mroute par interface ; Contrôle d'admission sur liaison Agg-DSLAM

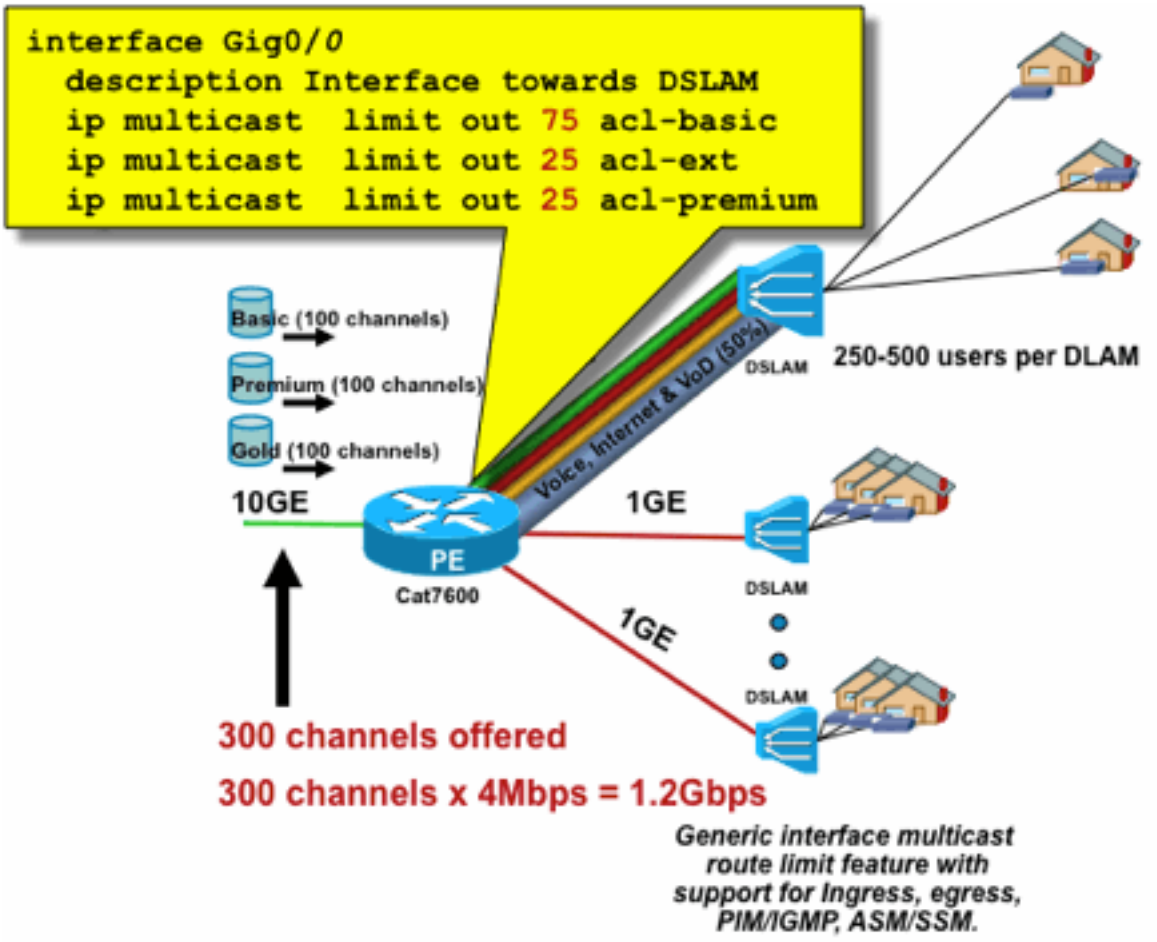

Fig21_PerInterface_Mroute

Exemple 2 : contrôle d'admission en entrée sur la liaison Agg-DSLAM

Au lieu de la limite « out » sur l'interface de sortie du périphérique en amont, il est possible d'utiliser des limites RPF sur l'interface RPF du périphérique en aval. Cela a effectivement le même résultat que l'exemple précédent et peut être utile si le périphérique en aval n'est pas un périphérique Cisco IOS.

Figure 22 : Utilisation des limites mroute par interface ; contrôle d'admission en entrée

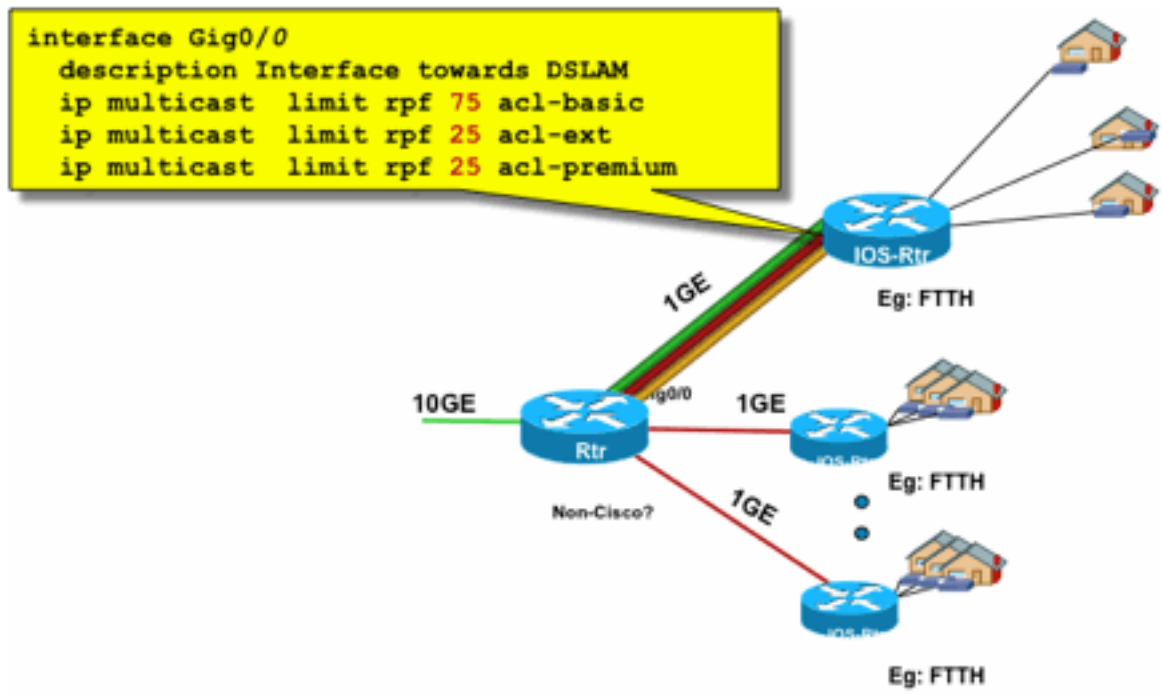

Fig22_PerInterface_Mroute_inputControl

Exemple 3 - Limites basées sur la bande passante

Vous pouvez subdiviser davantage la bande passante d'accès entre plusieurs fournisseurs de contenu et offrir à chaque fournisseur de contenu une part équitable de la bande passante sur la liaison montante vers le DSLAM. Dans ce cas, utilisez la commande **ip multicast limit cost** :

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

Avec cette commande, il est possible d'attribuer un « coût » (utilisez la valeur spécifiée dans « multiplicateur ») à tous les états qui correspondent à la liste de contrôle d'accès étendue dans la limite ip multicast.

Cette commande est globale et plusieurs coûts simultanés peuvent être configurés.

Dans cet exemple, il est nécessaire de prendre en charge trois fournisseurs de contenu différents avec un accès équitable à chacun dans le réseau. En outre, dans cet exemple, il est nécessaire de prendre en charge les flux MPEG (Moving Picture Experts Group) de différents types :

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

Dans ce cas, vous pouvez allouer des coûts de bande passante à chaque type de flux et partager le reste des 750 Mbits/s entre les trois fournisseurs de contenu avec cette configuration :

```
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
```

Figure 23 : Facteur de coût pour les limites d'état Mroute par interface

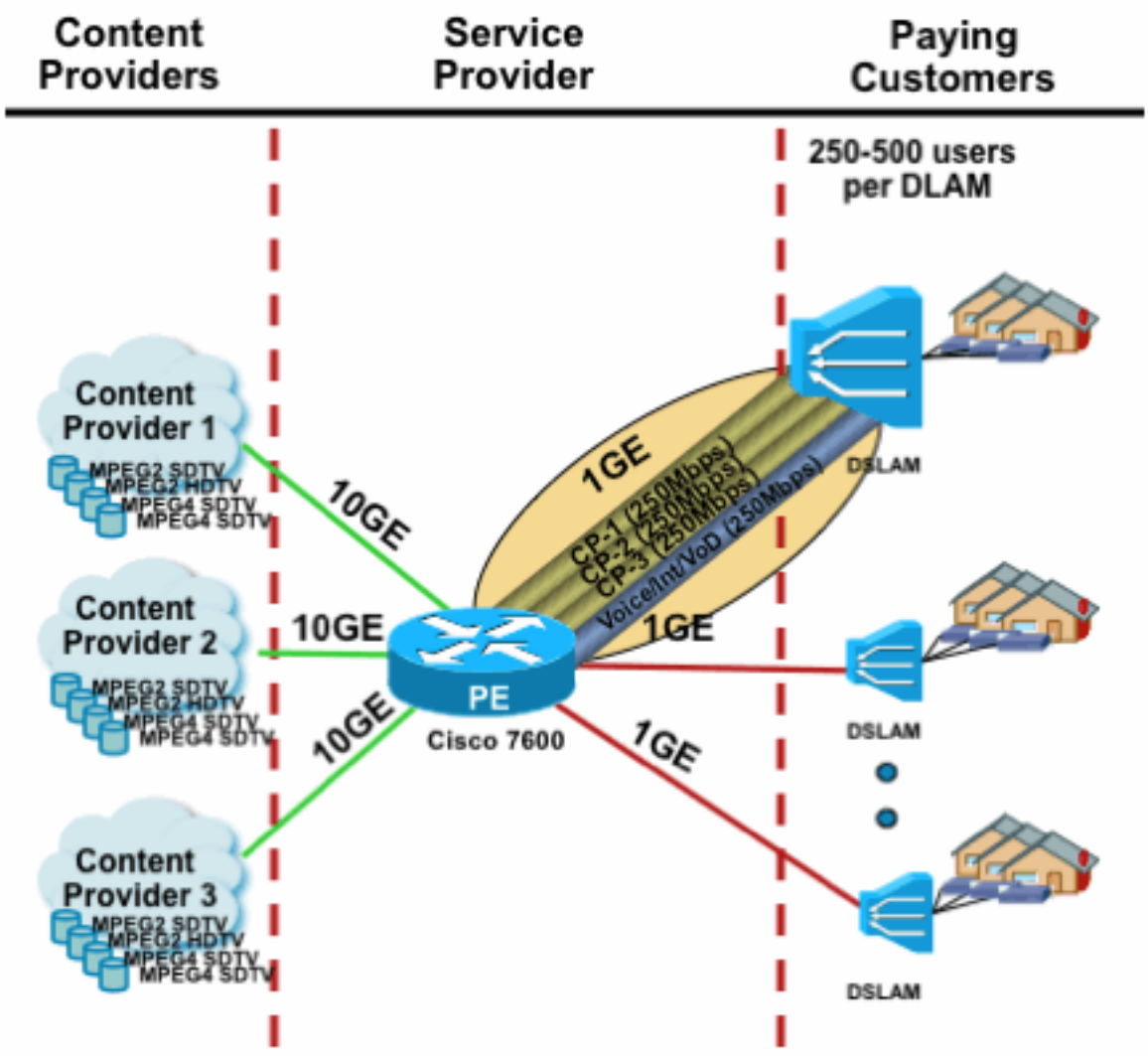

Fig23_Cost_PerInterface

Multidiffusion et IPSec

Présentation de GET VPN

Comme pour la monodiffusion, le trafic multidiffusion doit parfois être sécurisé pour assurer la confidentialité ou la protection de l'intégrité. Il y a deux grands domaines où de tels services pourraient être nécessaires :

- Cryptage des flux de multidiffusion (par exemple dans les applications bancaires qui transmettent des données confidentielles à un grand nombre de récepteurs qui utilisent la multidiffusion) : il s'agit de la sécurité du plan de données.
- Chiffrement des protocoles de plan de contrôle qui utilisent la multidiffusion, OSPF ou PIM, par exemple - il s'agit de la sécurité du plan de contrôle.

IPSec en tant que protocole [RFC 6040, 7619, 4302, 4303, 5282] est spécifiquement limité au

trafic de monodiffusion (par RFC). Là, une « association de sécurité » (SA) est établie entre deux homologues de monodiffusion. Afin d'appliquer IPSec au trafic de multidiffusion, une option est d'encapsuler le trafic de multidiffusion dans un tunnel GRE, puis d'appliquer IPSec au tunnel GRE, qui est unicast. Une approche plus récente utilise une association de sécurité unique établie entre tous les membres du groupe. Le domaine d'interprétation de groupe (GDOI) [RFC 6407] définit la manière d'y parvenir.

Basé sur GDOI, Cisco a développé une technologie appelée VPN GET (Group Encryption Transport). Cette technologie utilise le « mode tunnel avec conservation d'adresse », tel que défini dans le document « draft-ietf-msec-ipsec-extensions ». Dans GET VPN, une association de sécurité de groupe est d'abord établie entre tous les membres du groupe. Ensuite, le trafic est protégé, soit avec ESP (charge utile de sécurité encapsulée) ou AH (en-tête d'authentification), qui utilise le mode tunnel avec conservation d'adresse.

En résumé, GET VPN encapsule un paquet multicast qui utilise les informations d'adresse de l'en-tête d'origine, puis protège le paquet interne par rapport à la politique de groupe, avec un ESP, par exemple.

L'avantage de GET VPN est que le trafic de multidiffusion n'est pas du tout affecté par les mécanismes d'encapsulation de sécurité. Les adresses d'en-tête IP routées restent identiques à l'en-tête IP d'origine. Le trafic multidiffusion peut être sécurisé de la même manière avec ou sans GET VPN.

La stratégie appliquée aux noeuds GET VPN est définie de manière centralisée sur un serveur de clés de groupe et distribuée à tous les noeuds de groupe. Par conséquent, tous les noeuds de groupe ont la même stratégie et les mêmes paramètres de sécurité appliqués au trafic de groupe. À l’instar de l’IPSec standard, la stratégie de chiffrement définit le type de trafic à protéger de quelle manière. Cela permet d'utiliser GET VPN à diverses fins.

Utiliser GET VPN pour chiffrer le trafic du plan de données multidiffusion

La politique de chiffrement à l'échelle du réseau est définie sur le serveur de clés de groupe et distribuée aux terminaux GET VPN. La stratégie contient la stratégie IPSec (mode IPSec - ici : mode tunnel avec conservation de l'en-tête) et les algorithmes de sécurité à utiliser (par exemple AES). Elle contient également une stratégie qui décrit le trafic pouvant être sécurisé, tel que défini par une liste de contrôle d’accès.

GET VPN peut être utilisé pour le trafic de multidiffusion et de monodiffusion. Une stratégie de sécurisation du trafic de monodiffusion peut être définie par une liste de contrôle d’accès :

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

Cela permet de chiffrer tout le trafic avec une adresse IP source de 10/8 et une adresse IP de destination de 10/8. Tout autre trafic, par exemple, le trafic de 10/8 vers une autre adresse, serait ignoré par GET VPN.

L'application de GET VPN pour le trafic de multidiffusion est techniquement la même. Par exemple, cette entrée de contrôle d'accès (ACE) peut être utilisée pour sécuriser le trafic de n'importe quelle source vers les groupes de multidiffusion respectifs :

```
permit ip any 239.192.0.0 0.0.255.255
```

Cette stratégie correspond à toutes les sources (« any ») et à tous les groupes de multidiffusion commençant par 239.192. Le trafic vers d'autres groupes de multidiffusion n'est pas sécurisé.

> **Note**: Une grande attention doit être accordée à la construction de la liste de contrôle d'accès cryptographique. Le trafic de gestion, ou le trafic qui provient de l'extérieur du domaine GET VPN mais se termine à l'intérieur (c'est-à-dire le trafic qui passe un seul point d'extrémité de chiffrement), doit être exclu de la stratégie GDOI.

Les erreurs courantes sont :

- permit ip any 224.0.0.0 0.255.255.255 : Cela chiffre également le trafic OSPF et d'autres trafics de plan de contrôle, qui sont destinés à un routeur homologue, par exemple.
- Le trafic de gestion n'est pas exclu de la stratégie de chiffrement, qui se termine à l'intérieur du réseau. Cela inclut le trafic GDOI lui-même.

Utiliser GET VPN pour authentifier le trafic du plan de contrôle

Il est généralement recommandé d'authentifier le trafic du plan de contrôle, tel que les protocoles de routage, pour s'assurer que les messages proviennent d'un homologue de confiance. Ceci est relativement simple pour les protocoles de plan de contrôle qui utilisent la monodiffusion, comme BGP. Cependant, de nombreux protocoles de plan de contrôle utilisent le trafic multidiffusion. Exemples : OSPF, RIP et PIM. Pour obtenir la liste complète, reportez-vous au registre d'espace d'adressage multidiffusion IPv4 de l'IANA.

Certains de ces protocoles ont une authentification intégrée, comme RIP (Routing Information Protocol) ou EIGRP (Enhanced Interior Group Routing Protocol), d'autres s'appuient sur IPSec pour fournir cette authentification (par exemple OSPFv3, PIM). Dans ce dernier cas, GET VPN offre un moyen évolutif de sécuriser ces protocoles. Dans la plupart des cas, la condition est l'authentification des messages de protocole, ou en d'autres termes, la vérification qu'un message a été envoyé par un homologue de confiance. Cependant, GET VPN permet également le chiffrement de ces messages.

Pour sécuriser (généralement authentifier uniquement) un tel trafic de plan de contrôle, le trafic doit être décrit avec une liste de contrôle d'accès et inclus dans la stratégie GET VPN. Les détails dépendent du protocole à sécuriser, où une attention doit être portée à savoir si la liste de contrôle d'accès inclut le trafic qui ne passe qu'un noeud VPN GET entrant (qui est encapsulé), ou aussi un noeud de sortie.

Il existe deux manières fondamentales de sécuriser les protocoles PIM :

- **permit ip any 224.0.0.13 0.0.0.0** : Il s'agit du groupe de multidiffusion « Tous les routeurs PIM ». Cependant, cela ne sécurise pas les messages PIM monodiffusion
- **permit pim any any** : Cela sécurise le protocole PIM, indépendamment de l'utilisation de la multidiffusion ou de la monodiffusion

> **Note**: Les commandes sont fournies à titre d'exemples pour aider à expliquer un concept. Par exemple, il est nécessaire d'exclure certains protocoles PIM utilisés pour démarrer PIM, tels que BSR ou Auto-RP. Ces méthodes présentent certains avantages et inconvénients qui dépendent du déploiement. Pour plus d'informations, reportez-vous à la documentation spécifique sur la sécurisation de PIM avec GET VPN.

Conclusions

La multidiffusion est un service de plus en plus courant dans les réseaux. L'émergence des services IPTV dans les réseaux résidentiels/domestiques à large bande et l'évolution vers des applications de commerce électronique sur de nombreux marchés financiers mondiaux ne sont que deux exemples des exigences qui font de la multidiffusion une exigence absolue. La multidiffusion présente une grande variété de défis en termes de configuration, d'exploitation et de gestion. L'un des principaux défis est la sécurité.

Ce document a examiné une variété de façons dont la multidiffusion peut être sécurisée :

- Tout d'abord, examinez l'ensemble des plans de contrôle et de données de multidiffusion, afin d'expliquer en quoi les différences par rapport à la monodiffusion présentent de nouveaux défis en matière de sécurité.
- Ensuite, un examen des protocoles clés rencontrés dans un réseau de multidiffusion, en particulier IGMP, PIM et MSDP ont été examinés en détail. Dans chaque cas, une description des menaces de sécurité et des meilleures pratiques recommandées pour les atténuer ont été fournies.
- En outre, certains exemples spécifiques montrent comment la multidiffusion peut être sécurisée dans certaines applications spécifiques, telles que les réseaux de périphérie à large bande, où la bande passante peut être limitée par rapport à la quantité de bande passante que des flux vidéo spécifiques pourraient nécessiter.
- Enfin, l'architecture GET VPN a été décrite comme un moyen de multidiffusion intégrée avec IPSec pour la fourniture de VPN sécurisés.

En gardant à l'esprit la sécurité de la multidiffusion, rappelez-vous qu'elle est différente de la monodiffusion. La transmission multidiffusion est basée sur la création d'un état dynamique, la multidiffusion implique une réplication de paquets dynamique et la multidiffusion crée des arborescences unidirectionnelles en réponse aux messages PIM JOIN / PRUNE. La sécurité de cet environnement implique la compréhension et le déploiement d'un cadre riche de commandes Cisco IOS. Ces commandes sont principalement centrées sur la protection des opérations de protocole, des états (multidiffusion) ou des régulateurs placés contre des paquets tels que CoPP. Une utilisation correcte de ces commandes permet de fournir un service protégé robuste pour la multidiffusion IP.

En résumé, plusieurs approches sont promues et décrites dans ce document :

1. Utilisation étendue du SSM : il s'agit du mode PIM le plus simple qui permet également l'utilisation du transfert (S, G).
2. Si des services ASM sont nécessaires, assurez-vous qu'un service robuste peut être fourni - l'utilisation de RP définis statiquement fournit un plan de contrôle plus sécurisé que les annonces RP dynamiques. Auto-RP et BSR sont plus flexibles
3. Si PIM-SM est activé, examinez les zones de vulnérabilité particulière, comme le tunnel de registre vers le RP, et assurez-vous que le DR est toujours bien protégé. La CoPP est très utile dans ces domaines.
4. Si des services ASM entre domaines sont nécessaires, déterminez si le protocole PIM BiDir peut être déployé.
5. Utiliser les limites d'état globales mroute/igmp - comprendre les capacités de vos plates-formes ainsi que la quantité maximale d'état attendue dont vous avez besoin dans des

circonstances normales et dans le pire des cas. Configurez des limites dans les capacités de votre plate-forme qui permettent à votre réseau de fonctionner à ses limites maximales.

6. Filtres fondamentaux : rACL/CoPP et ACL d'infrastructure, qui bloquent le protocole PIM au niveau de la couche d'accès

La multidiffusion IP est un moyen intéressant et évolutif de fournir une variété de services d'application. Comme la monodiffusion, elle doit être sécurisée dans une variété de zones différentes. Ce document fournit les éléments de base qui peuvent être utilisés pour sécuriser un réseau de multidiffusion IP.

Informations connexes

- Instructions d'allocation d'adresses de multidiffusion IP d'entreprise
- Configuration des filtres IGMP IPv4
- Group Encrypted Transport VPN

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.