

Routage multidiffusion

Ce chapitre décrit comment configurer ASA pour utiliser le protocole de routage de multidiffusion.

- Routage multidiffusion, à la page 1
- Lignes directrices pour le routage de multidiffusion, à la page 5
- Routage multidiffusion activé, à la page 6
- Personnaliser le routage multidiffusion, à la page 7
- Supervision de PIM, à la page 23
- Exemple de routage de multidiffusion, à la page 23
- Historique du routage de multidiffusion, à la page 25

Routage multidiffusion

Le routage de multidiffusion est une technologie de conservation de la bande passante qui réduit le trafic en délivrant simultanément un seul flux d'informations à des milliers d'entreprises et de domiciles. Les applications comprennent les vidéoconférences, les communications d'entreprise, l'apprentissage à distance et la distribution de logiciels, de cotations boursières et d'actualités.

Applications et protocoles de routage de multidiffusion

Les protocoles de routage de multidiffusion envoient efficacement le trafic source à plusieurs destinataires, sans ajouter de charge supplémentaire sur la source ou les destinataires, et utilisent moins de bande passante réseau que les autres technologies. Les paquets en multidiffusion sont répliqués dans le réseau par l'activation de l'ASA avec PIM (Protocol Independent Multicast) et d'autres protocoles de multidiffusion qui prennent en charge, ce qui permet la livraison la plus efficace possible des données à plusieurs destinataires.

L'ASA prend en charge le routage de multidiffusion stub et le routage de multidiffusion PIM. Cependant, vous ne pouvez pas configurer les deux simultanément sur un seul ASA.

Remarque Les transports UDP et non-UDP sont tous deux pris en charge pour le routage de multidiffusion. Cependant, le transport non UDP n'a pas d'optimisation FastPath.

Routage de multidiffusion en mode stub

Le routage de multidiffusion tampon permet un enregistrement dynamique de l'hôte et facilite le routage de multidiffusion.

Lorsqu'il est configuré pour le routage de multidiffusion stub, l'ASA agit comme un agent mandataire IGMP. Au lieu de participer entièrement au routage de multidiffusion, l'ASA transfère les messages IGMP à un routeur de multidiffusion en amont, qui configure la livraison des données en multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion tampon, l'ASA ne peut pas être configuré pour le mode PIM discret ou bidirectionnel. Activez PIM sur les interfaces qui participent au routage de multidiffusion en mode stub IGMP.

L'ASA prend en charge PIM-SM et PIM bidirectionnel. PIM-SM est un protocole de routage de multidiffusion qui utilise la base d'information de routage sous-jacente de monodiffusion ou une base d'information de routage distincte compatible avec la multidiffusion. Il crée des arborescences partagées unidirectionnelles, chacune ayant pour racine un seul point de rendez-vous (PRV) par groupe de multidiffusion. Il crée éventuellement des arborescences de plus court chemin pour chaque source de multidiffusion.

Routage de multidiffusion PIM

Le PIM bidirectionnel est une variante de PIM-SM qui crée des arborescences partagées bidirectionnelles connectant les sources et les récepteurs de multidiffusion.

Processus d'élection du DF

Les arborescences bidirectionnelles sont créées à l'aide d'un processus de sélection de désigné de transitaire (DF) qui fonctionne sur chaque lien de la topologie de multidiffusion. Avec l'aide du DF, les données en multidiffusion sont transmises des sources au point de rendez-vous (RP), et donc le long de l'arborescence partagée jusqu'aux récepteurs. Ce processus ne nécessite pas d'état spécifique à la source. Le choix du DF a lieu lors de la découverte du RP et fournit une voie de routage par défaut vers le RP.



Remarque Si ASA est le RP du PIM, utilisez l'adresse externe non traduite de l'ASA comme adresse RP.

Mode PIM clairsemé

Le mode clairsemé (PIM-SM) est un mode PIM qui transfère le trafic uniquement lorsqu'il est spécifiquement demandé par les destinataires. Il utilise un point de rendez-vous (PRV) central pour coordonner le transfert du trafic de multidiffusion entre la source de multidiffusion et la destination. Le PRV est un routeur qui sert de point de rencontre pour la source et les destinataires. Les sources de multidiffusion s'enregistrent auprès du PRV par l'intermédiaire de leur routeur de premier saut. Ils envoient une copie du trafic de multidiffusion aux destinataires par l'intermédiaire du PRV.

Prise en charge de la multidiffusion PIM propre à la source

ASA peut transférer le trafic de multidiffusion spécifique à la source (p. ex., pour les groupes dans la plage 232.xxx) même s'il ne prend pas en charge la configuration PIM-SSM ou le protocole de gestion de groupes Internet version 3 (IGMPv3).

SSM est classé comme un mécanisme de livraison de données pour les applications un-à-plusieurs telles que l'IPTV. Le modèle SSM utilise un concept de « canaux » désigné par une paire (S, G), où S est une adresse de source et G une adresse de destination SSM. L'abonnement à un canal se fait à l'aide d'un protocole de gestion de groupe comme IGMPv3. SSM permet à un client destinataire, une fois qu'il a pris connaissance d'une source en multidiffusion particulière, de recevoir des flux en multidiffusion directement de la source plutôt que de les recevoir d'un point de rendez-vous partagé (RP). Des mécanismes de contrôle d'accès ont été introduits dans SSM pour fournir une amélioration de la sécurité non disponible avec les implémentations actuelles en mode clairsemé ou dense.

Limites :

- ASA ne peut pas servir de routeur de dernier saut pour la multidiffusion SSM, car il ne prend pas en charge IGMPv3 (que les destinataires utilisent pour joindre des groupes SSM).

  Si l'ASA est le dernier saut, il ignorera les messages de jonction IGMPv3 des destinataires pour les groupes SSM, et le transfert SSM ne fonctionnera pas.

- Les voies de routage de multidiffusion statiques sur ASA ne fonctionnent pas pour la plage SSM (232.x.x.x).

Solution de rechange:

Pour que le pare-feu Cisco ASA transfère le trafic de multidiffusion lié à SSM, vous devez ajouter un périphérique de couche 3 compatible avec la multidiffusion (comme un routeur ou un commutateur) qui prend en charge PIM et IGMPv3 sur le même segment de réseau que les récepteurs.

Modalités de fonctionnement :

- Les destinataires enregistrent leurs demandes d'adhésion aux groupes SSM (IGMPv3) auprès de ce périphérique de couche 3.
- Ce périphérique de couche 3 envoie des messages de jonction PIM vers l'ASA.
- L'ASA reçoit ces messages PIM et apprend dynamiquement les voies de routage de multidiffusion.
- Le trafic de multidiffusion SSM est ensuite correctement acheminé par l'ASA, car il ne s'agit plus du périphérique de dernier saut.

Routeur de démarrage PIM (BSR)

PIM Bootstrap Router (BSR) est un modèle de sélection dynamique des Points de Rendez vous (RP) qui utilise des routeurs candidats pour la fonction RP et pour le relais des informations RP pour un groupe.

La fonction RP comprend la découverte de RP et fournit une voie de routage par défaut vers le RP. Pour ce faire, elle configure un ensemble de périphériques en tant que candidats BSR (C-BSR) qui participent à un processus de sélection d'un BSR pour choisir un BSR parmi eux. Une fois le BSR choisi, les périphériques configurés en tant que points de rendez-vous candidats (C-RP) commencent à envoyer leur mappage de groupe au BSR élu. Le BSR distribue ensuite les informations de mappage groupe-RP à tous les autres périphériques en aval dans l'arborescence de multidiffusion par l'intermédiaire de messages du BSR qui voyagent de routeur PIM à routeur PIM par saut.

Cette fonctionnalité permet aux réseaux de découvrir dynamiquement les RP. La découverte dynamique des RP est essentielle dans les réseaux vastes et complexes où un RP peut occasionnellement tomber en panne puis redevenir opérationnel.

Terminologie du routeur de démarrage PIM (BSR)

Cette référence fournit des définitions des termes clés utilisés dans les configurations des routeurs de démarrage PIM (BSR) pour aider à comprendre les rôles et les fonctions des différents composants dans le processus d'élection de BSR et d'annonce de RP.

Les termes suivants sont fréquemment mentionnés dans la configuration du BSR PIM :

- Routeur Bootstrap (BSR) : un BSR annonce des informations de point de rendez-vous (RP) à d'autres routeurs avec PIM saut par saut. Parmi plusieurs candidats BSR, un seul BSR est choisi à l'issue d'un processus de sélection. L'objectif principal de ce routeur Bootstrap est de collecter toutes les annonces de Candidat RP (C-RP) dans une base de données appelée RP-set et de les envoyer périodiquement à tous les autres routeurs du réseau en tant que messages BSR (toutes les 60 secondes) .
- Messages Bootstrap Router (BSR) : les messages BSR sont en multidiffusion vers le groupe All-PIM-Routers avec une TTL de 1. Tous les voisins PIM qui reçoivent ces messages les retransmettent (encore une fois avec une TTL de 1) sur toutes les interfaces, à l'exception de celle dans laquelle les messages ont été reçus. Les messages BSR contiennent l'ensemble de RP et l'adresse IP du BSR actuellement actif. Voici comment les C-RP savent où envoyer en monodiffusion leurs messages C-RP.
- Candidate Bootstrap Router (C-BSR) : un appareil configuré en tant que candidat-BSR participe au mécanisme de sélection du BSR. Un C-BSR de priorité la plus élevée est choisi comme BSR. L'adresse IP la plus élevée de C-BSR est utilisée comme condition de départage. Le processus de sélection BSR est préemptif, par exemple, si un nouveau C-BSR avec une priorité plus élevée se présente, il déclenche un nouveau processus de sélection.
- Point de rendez-vous candidat (C-RP) : un RP sert de point de rencontre pour les sources et les récepteurs des données de multidiffusion. Un périphérique configuré en tant que C-RP annonce périodiquement les informations de mappage de groupe de multidiffusion directement au BSR choisi par la monodiffusion. Ces messages contiennent la plage de groupe, l'adresse C-RP et une durée d'attente. L'adresse IP du BSR actuel est apprise à partir des messages périodiques du BSR reçus par tous les routeurs du réseau. De cette façon, le BSR apprend quels sont les RP possibles qui sont actuellement actifs et accessibles.



Remarque L'ASA n'agit pas comme un C-RP, même si le C-RP est une exigence obligatoire pour le trafic BSR. Seuls les routeurs peuvent agir en tant que C-RP. Ainsi, pour la fonctionnalité de test du BSR, vous devez ajouter des routeurs à la topologie.

- Mécanisme de sélection BSR – Chaque C-BSR génère des messages Bootstrap (BSM) qui contiennent un champ de priorité BSR. Les routeurs du domaine inondent les BSM dans tout le domaine. Un C-BSR qui entend parler d'un C-BSR de priorité plus élevée que lui supprime l'envoi d'autres BSM pendant un certain temps. L'unique C-BSR restant devient le BSR élu, et ses BSM informent tous les autres routeurs du domaine qu'il est le BSR choisi.

Concept de groupe de multidiffusion

La multidiffusion est basée sur le concept de groupe. Un groupe arbitraire de récepteurs souhaite recevoir un flux de données particulier. Ce groupe n'a aucune limite physique ou géographique. Les hôtes peuvent être situés n'importe où sur Internet. Les hôtes qui souhaitent recevoir des données envoyées à un groupe doivent rejoindre le groupe à l'aide d'IGMP.

Exigences d'appartenance au groupe

Les hôtes doivent être membres du groupe pour recevoir le flux de données. Pour en savoir plus sur la configuration des groupes de multidiffusion, consultez Configurer un groupe de multidiffusion, à la page 18.

Adresses de multidiffusion

Les adresses de multidiffusion spécifient un groupe quelconque d'hôtes IP qui ont rejoint le groupe et qui souhaitent recevoir le trafic envoyé à ce groupe.

Mise en grappe

Le routage de multidiffusion prend en charge la mise en grappe. Dans la mise en grappe étendue EtherChannel, l'unité de contrôle envoie tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi.

Une fois le transfert rapide établi, les unités de données peuvent transférer des paquets de données en multidiffusion. Tous les flux de données sont des flux complets. Les flux de transfert des tampons sont également pris en charge. Comme une seule unité reçoit les paquets en multidiffusion dans une grappe EtherChannel étendue, la redirection vers l'unité de contrôle est courante. Dans le regroupement d'interfaces individuelles, les unités n'agissent pas indépendamment. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle. Les unités de données abandonnent tous les paquets qui ont été envoyés.

Lignes directrices pour le routage de multidiffusion

Tableau 1 : Configuration système requise

Article	Description
Mode contextuel	Pris en charge en mode contexte unique
Mode pare-feu	Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.
IPv6	IPv6 n'est pas pris en charge.
Groupe de multidiffusion	La plage d'adresses entre 224.0.0.0 et 224.0.0.255 est réservée pour l'utilisation des protocoles de routage et d'autres protocoles de découverte ou de maintenance de topologie, tels que la découverte de passerelle et les rapports sur les membres de groupes. Le routage de multidiffusion Internet à partir de la plage d'adresses 224.0.0/24 n'est pas pris en charge. Lorsque le routage de multidiffusion est activé pour les adresses réservées, aucun groupe IGMP n'est créé.
Mise en grappes	En grappe, pour IGMP et PIM, cette fonctionnalité n'est prise en charge que sur l'unité principale.

Configuration du contrôle d'accès

Vous devez configurer une règle de contrôle d'accès sur l'interface entrante pour autoriser le trafic vers l'hôte de multidiffusion, comme l'interface 224.1.2.3. Cependant, vous ne pouvez pas spécifier une interface de destination pour la règle, ou elle ne peut pas être appliquée aux connexions en multidiffusion lors de la validation initiale de la connexion.

Gestion des interfaces et des protocoles

Assurez-vous d'une bonne gestion de la configuration lorsque vous utilisez des interfaces compatibles avec PIM et des protocoles de routage de multidiffusion.

- Le routage de multidiffusion n'est pas pris en charge dans ECMP.
- Ne configurez pas ASA pour être à la fois un point de rendez-vous (RP) et un routeur de premier saut.
- L'adresse IP de secours HSRP ne participe pas au voisinage PIM. Ainsi, si l'adresse IP du routeur PRV est acheminée par l'intermédiaire d'une adresse IP de secours HSRP, le routage de multidiffusion ne fonctionne pas dans ASA. Pour que le trafic en multidiffusion soit acheminé correctement, configurez la voie de routage vers l'adresse du PRV pour qu'elle utilise une adresse IP d'interface plutôt que l'adresse IP de secours HSRP.

Routage multidiffusion activé

L'activation du routage de multidiffusion sur l'ASA active l'IGMP et la PIM sur toutes les interfaces de données par défaut, mais pas sur l'interface de gestion pour la plupart des modèles (voir L'interface de logement/port de gestion pour les interfaces qui n'autorisent pas le trafic). IGMP est utilisé pour savoir si les membres d'un groupe sont présents sur les sous-réseaux directement associés. Les hôtes se joignent aux groupes de multidiffusion en envoyant des messages de rapport IGMP. PIM est utilisé pour maintenir les tableaux de transfert pour transférer les datagrammes en multidiffusion.

Pour activer le routage de multidiffusion sur l'interface de gestion, vous devez définir explicitement une limite de multidiffusion sur l'interface de gestion.

Remarque Seule la couche de transport UDP est prise en charge pour le routage de multidiffusion.

La liste suivante indique le nombre maximal d'entrées pour des tableaux de multidiffusion spécifiques. Une fois ces limites atteintes, toute nouvelle entrée est rejetée.

- MFIB : 30 000
- Groupes IGMP : 30 000
- Routages PIM : 72 000

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)**.

Étape 2 Dans le volet Multicast (Multidiffusion), cochez la case **Enable Multicast routing** (Activer le routage de multidiffusion).

Cochez cette case pour activer le routage de multidiffusion IP sur l'ASA. Décocher cette case désactive le routage de multidiffusion IP. Par défaut, la multidiffusion est désactivée. L'activation du routage de multidiffusion active la multidiffusion sur toutes les interfaces. Vous pouvez désactiver la multidiffusion interface par interface.

Personnaliser le routage multidiffusion

Cette section décrit comment personnaliser le routage multidiffusion.

Configurer le routage de multidiffusion Stub et transférer les messages IGMP



Remarque Le routage de multidiffusion de stub n'est pas pris en charge en même temps que les modes fragmenté et bidirectionnel de la PIM.

Un ASA agissant en tant que passerelle vers la zone de stub n'a pas besoin de participer au mode fractionné (PIM) ou au mode bidirectionnel. Au lieu de cela, vous pouvez le configurer pour qu'il agisse comme un agent mandataire et transfère les messages IGMP des hôtes connectés sur une interface vers un routeur de multidiffusion en amont sur une autre interface. Pour configurer l'ASA en tant qu'agent de mandataire IGMP, transférez les messages de jonction et de sortie de l'hôte de l'interface de zone de stub vers une interface en amont. Vous devez également activer la PIM sur les interfaces qui participent au routage de multidiffusion en mode stub.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)**.

Étape 2 Dans le volet Multicast (Multidiffusion), cochez la case **Enable Multicast routing** (Activer le routage de multidiffusion).

Étape 3 Cliquez sur **Apply** pour enregistrer vos modifications.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 5 Pour modifier l'interface à partir de laquelle vous souhaitez transférer les messages IGMP, sélectionnez l'interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Configure IGMP Parameters** (Configurer les paramètres IGMP) apparaît.

Étape 6 Dans la liste déroulante **Forward Interface** (Interface de transfert), choisissez l'interface spécifique à partir de laquelle vous souhaitez transférer les messages IGMP.

Étape 7 Cliquez sur **OK** pour fermer cette boîte de dialogue, puis cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications.

Configurer une route de multidiffusion statique

La configuration de routes statiques de multidiffusion vous permet de séparer le trafic de multidiffusion du trafic de monodiffusion. Par exemple, quand un chemin entre une source et une destination ne prend pas en charge le routage de multidiffusion, la solution consiste à configurer deux périphériques de multidiffusion avec un tunnel GRE et d'envoyer les paquets en multidiffusion sur le tunnel.

Lors de l'utilisation de PIM, l'ASA s'attend à recevoir des paquets sur la même interface où il renvoie les paquets de monodiffusion à la source. Dans certains cas, par exemple pour contourner une voie de routage qui ne prend pas en charge le routage de multidiffusion, vous pouvez souhaiter que les paquets monodiffusion prennent un chemin et les paquets multidiffusion, un autre.

Les routes de multidiffusion statiques ne sont pas annoncées ou redistribuées.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **MRoute**.

Étape 2 Choisissez **Add** (Ajouter) ou **Edit** (Modifier).

La boîte de dialogue Add or Edit Multicast Route (Ajouter ou modifier une route de multidiffusion) s'affiche.

Utilisez la boîte de dialogue Add Multicast Route (Ajouter une route de multidiffusion) pour ajouter une nouvelle route de multidiffusion statique à l'ASA. Utilisez la boîte de dialogue Edit Multicast Route (Modifier une route de multidiffusion) pour modifier une route de multidiffusion statique existante.

Étape 3 Dans le champ Source Address (Adresse source), saisissez l'adresse IP de la source de multidiffusion. Vous ne pouvez pas modifier cette valeur lors de la modification d'une route de multidiffusion statique existante.

Étape 4 Choisissez le masque réseau pour l'adresse IP de la source de multidiffusion dans la liste déroulante Source Mask (Masque source).

Étape 5 Dans la zone Incoming Interface (Interface entrante), cliquez sur le bouton radio **RPF Interface** (Interface RPF) pour choisir RPF pour transférer le routage ou sur le bouton radio **Interface Name** (Nom de l'interface), puis saisissez la commande suivante :

- Dans le champ Source Interface (Interface source), choisissez l'interface entrante pour la route de multidiffusion dans la liste déroulante.
- Dans le champ Destination Interface (Interface de destination), choisissez l'interface de destination par laquelle la route est transférée dans la liste déroulante.

Remarque Vous pouvez spécifier l'interface ou le voisin RPF, mais pas les deux en même temps.

Étape 6 Dans le champ Administrative Distance (Distance administrative), choisissez la distance administrative de la route de multidiffusion statique. Si la route de multidiffusion statique a la même distance administrative que la route de monodiffusion, la route de multidiffusion statique prévaut.

Étape 7 Cliquez sur **OK**.

Configurer des fonctionnalités IGMP

Les hôtes IP utilisent le protocole IGMP pour signaler leur appartenance à des groupes aux routeurs de multidiffusion connectés directement. IGMP est utilisé pour enregistrer dynamiquement des hôtes individuels dans un groupe de multidiffusion sur un réseau local particulier. Les hôtes déterminent les appartenances aux groupes en envoyant des messages IGMP à leur routeur de multidiffusion local. Sous IGMP, les routeurs écoutent les messages IGMP et envoient périodiquement des requêtes pour découvrir quels groupes sont actifs ou inactifs sur un sous-réseau particulier.

Cette section décrit comment configurer les paramètres IGMP facultatifs pour l'interface.

Désactiver IGMP sur une interface

Vous pouvez désactiver IGMP sur des interfaces spécifiques. Cela est utile si vous savez qu'il n'y a aucun hôte en multidiffusion sur une interface spécifique et que vous souhaitez empêcher l'ASA d'envoyer des messages de requête d'hôte sur cette interface.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Le volet Protocol (Protocole) affiche les paramètres IGMP pour chaque interface de l'ASA.

Étape 2 Sélectionnez l'interface que vous souhaitez désactiver et cliquez sur **Edit** (Modifier).

Étape 3 Pour désactiver l'interface spécifiée, décochez la case **Enable IGMP** (Activer IGMP).

Étape 4 Cliquez sur **OK**.

Le volet Protocol (Protocole) affiche Yes (Oui) si IGMP est activé sur l'interface ou No (Non) si IGMP est désactivé sur l'interface.

Configurer l'appartenance au groupe IGMP

Vous pouvez configurer l'ASA pour qu'il soit membre d'un groupe de multidiffusion. La configuration de l'ASA pour se joindre à un groupe de multidiffusion fait en sorte que les routeurs en amont conservent les renseignements de la table de routage de multidiffusion pour ce groupe et maintiennent les chemins de ce groupe actifs.

Remarque Si vous souhaitez transférer des paquets en multidiffusion pour un groupe spécifique vers une interface sans que l'ASA n'accepte ces paquets dans le cadre du groupe, consultez Configurer un groupe IGMP joint statiquement, à la page 10.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Join Group (Groupe de jonction)**.

Étape 2 Cliquez sur **Add** (Ajouter) ou **Edit** > **(Modifier) dans le volet** > **Join Group** > **(Groupe de jonction)**.

La boîte de dialogue Add IGMP Join Group (Ajouter un groupe de jonction IGMP) vous permet de configurer une interface pour qu'elle soit membre d'un groupe de multidiffusion. La boîte de dialogue Edit IGMP Join Group (Modifier un groupe de jonction IGMP) vous permet de modifier les renseignements d'appartenance existants.

Étape 3 Dans le champ Interface Name (Nom de l'interface), choisissez le nom de l'interface dans la liste déroulante. Si vous modifiez une entrée existante, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse d'un groupe de multidiffusion auquel appartient l'interface. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.

Étape 5 Cliquez sur **OK**.

Configurer un groupe IGMP joint statiquement

Parfois, un membre d'un groupe ne peut pas signaler son appartenance au groupe en raison d'une configuration, ou il se peut qu'il n'y ait aucun membre d'un groupe sur le segment de réseau. Cependant, vous souhaitez toujours que le trafic de multidiffusion de ce groupe soit envoyé vers ce segment de réseau. Vous pouvez envoyer le trafic de multidiffusion pour ce groupe au segment en configurant un groupe IGMP rejoint statiquement.

Dans la fenêtre principale d'ASDM, choisissez **Configuration > Routing (Routage) > Multicast (Multidiffusion) > IGMP > Static Group (Groupe statique)** pour configurer l'ASA en tant que membre connecté de manière statique à un groupe. Avec cette méthode, l'ASA n'accepte pas les paquets lui-même, mais les transfère seulement. Par conséquent, cette méthode permet une commutation rapide. L'interface sortante apparaît dans le cache IGMP, mais cette interface n'est pas membre du groupe de multidiffusion.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Static Group (Groupe statique)**.

Étape 2 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans le volet **Static Group** (Groupe statique).

Utilisez la boîte de dialogue Add IGMP Static Group (Ajouter un groupe statique IGMP) pour affecter de manière statique un groupe de multidiffusion à une interface. Utilisez la boîte de dialogue Edit IGMP Static Group (Modifier un groupe statique IGMP) pour modifier les affectations de groupes statiques existantes.

Étape 3 Dans le champ Interface Name (Nom de l'interface), choisissez le nom de l'interface dans la liste déroulante. Si vous modifiez une entrée existante, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse d'un groupe de multidiffusion auquel appartient l'interface. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.

Étape 5 Cliquez sur **OK**.

Contrôler l'accès aux groupes de multidiffusion

Vous pouvez contrôler l'accès aux groupes de multidiffusion à l'aide de listes de contrôle d'accès.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Access Group (Groupe d'accès)**.

Le volet Access Group (Groupe d'accès) apparaît. Les entrées du tableau dans le volet Access Group (Groupe d'accès) sont traitées de haut en bas. Placez les entrées plus spécifiques en haut du tableau et les entrées plus génériques plus bas. Par exemple, placez une entrée de groupe d'accès qui autorise un groupe de multidiffusion spécifique près du haut du tableau et une entrée de groupe d'accès en dessous qui refuse une plage de groupes de multidiffusion, y compris le groupe dans la règle d'autorisation. Le groupe est autorisé car la règle d'autorisation est appliquée avant la règle de refus.

Un double-clic sur une entrée du tableau ouvre la boîte de dialogue Add or Edit Access Group (Ajouter ou modifier un groupe d'accès) pour l'entrée sélectionnée.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

La boîte de dialogue Add Access Group (Ajouter un groupe d'accès) ou Edit Access Group (Modifier un groupe d'accès) apparaît. La boîte de dialogue Add Access Group (Ajouter un groupe d'accès) vous permet d'ajouter un nouveau groupe d'accès au tableau des groupes d'accès. La boîte de dialogue Edit Access Group (Modifier un groupe d'accès) vous permet de modifier les renseignements d'une entrée de groupe d'accès existante. Certains champs peuvent être grisés lors de la modification des entrées existantes.

Étape 3 Choisissez le nom d'interface auquel le groupe d'accès est associé dans la liste déroulante Interface. Vous ne pouvez pas modifier l'interface associée lorsque vous modifiez un groupe d'accès existant.

Étape 4 Choisissez permit (autoriser) dans la liste déroulante Action pour autoriser le groupe de multidiffusion sur l'interface sélectionnée. Choisissez deny (refuser) dans la liste déroulante Action pour filtrer le groupe de multidiffusion de l'interface sélectionnée.

Étape 5 Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse du groupe de multidiffusion auquel le groupe d'accès s'applique.

Étape 6 Saisissez le masque réseau pour l'adresse du groupe de multidiffusion ou sélectionnez l'un des masques réseau courants dans la liste déroulante Netmask (Masque réseau).

Étape 7 Cliquez sur **OK**.

Limiter le nombre d'états IGMP sur une interface

Vous pouvez limiter le nombre d'états IGMP résultant des rapports sur les membres IGMP pour chaque interface. Les rapports sur les membres dépassant les limites configurées ne sont pas entrés dans la mémoire cache IGMP et le trafic pour les rapports sur les membres excédentaires n'est pas transféré.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez limiter dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Configure IGMP Parameters (Configurer les paramètres IGMP) apparaît.

Étape 3 Dans le champ Group Limit (Limite de groupe), saisissez le nombre maximum d'hôtes qui peuvent rejoindre une interface.

La valeur par défaut est 500. Les valeurs valides sont comprises entre 0 et 5 000.

Remarque La définition de cette valeur à 0 empêche l'ajout de groupes appris, mais les appartenances définies manuellement sont toujours autorisées.

Étape 4 Cliquez sur **OK**.

Remarque Lorsque vous modifiez la limite IGMP sur l'interface avec des jonctions actives, la nouvelle limite ne s'applique pas aux groupes existants. L'ASA valide la limite uniquement lorsqu'un nouveau groupe est ajouté à l'interface ou lorsque les minuteries de jonction IGMP expirent. Pour appliquer la nouvelle limite avec effet immédiat, vous devez désactiver et réactiver IGMP sur l'interface.

Modifier les messages de requête destinés aux groupes de multidiffusion

L'ASA envoie des messages de requête pour découvrir quels groupes de multidiffusion ont des membres sur les réseaux connectés aux interfaces. Les membres répondent par des messages de rapport IGMP indiquant qu'ils souhaitent recevoir des paquets en multidiffusion pour des groupes spécifiques. Les messages de requête sont adressés au groupe de multidiffusion tous les systèmes, qui possède l'adresse 224.0.0.1 et une valeur de durée de vie de 1.

Ces messages sont envoyés périodiquement pour actualiser les renseignements sur les membres stockés sur l'ASA. Si l'ASA découvre qu'il n'y a aucun membre local d'un groupe de multidiffusion connecté à une

interface, il arrête de transférer le paquet en multidiffusion pour ce groupe vers le réseau connecté et il renvoie un message d'élaguer à la source des paquets.

Par défaut, le routeur désigné PIM sur le sous-réseau est responsable de l'envoi des messages de requête. Par défaut, ils sont envoyés toutes les 125 secondes.

Lors de la modification du temps de réponse aux requêtes, par défaut, le temps de réponse maximal aux requêtes annoncé dans les requêtes IGMP est de 10 secondes. Si l'ASA ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.

Pour modifier l'intervalle de requête, le temps de réponse à la requête et la valeur du délai d'expiration de la requête, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez limiter dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Configure IGMP Parameters (Configurer les paramètres IGMP) apparaît.

Étape 3 Dans le champ **Query Interval** (Intervalle de requête), saisissez l'intervalle en secondes auquel le routeur désigné envoie des messages de requête d'hôte IGMP.

Les valeurs valides vont de 1 à 3 600 secondes. La valeur par défaut est 125 secondes.

Remarque Si l'ASA n'entend pas de message de requête sur une interface pendant le délai d'expiration spécifié, l'ASA devient le routeur désigné et commence à envoyer les messages de requête.

Étape 4 Dans le champ **Query Timeout** (Délai d'expiration de la requête), saisissez la période en secondes avant laquelle l'ASA prend le relais en tant que demandeur pour l'interface après l'arrêt du demandeur précédent.

Les valeurs valides vont de 60 à 300 secondes. La valeur par défaut est 255secondes.

Étape 5 Dans le champ **Response Time** (Temps de réponse), saisissez le temps de réponse maximum annoncé dans les requêtes IGMP, en secondes.

Les valeurs sont comprises entre 1 et 25 secondes. La valeur par défaut est 10 secondes.

Étape 6 Cliquez sur **OK**.

Modifier la version IGMP

Par défaut, l'ASA exécute la version 2 du protocole IGMP, qui active plusieurs fonctionnalités supplémentaires.

Tous les routeurs de multidiffusion d'un sous-réseau doivent prendre en charge la même version d'IGMP. L'ASA ne détecte pas automatiquement les routeurs de la version 1 et passe à la version 1. Cependant, une combinaison d'hôtes IGMP versions 1 et 2 sur le sous-réseau fonctionne; l'ASA exécutant IGMP version 2 fonctionne correctement lorsque des hôtes IGMP version 1 sont présents.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface dont vous souhaitez modifier la version d'IGMP dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Configure IGMP Interface (Configurer l'interface IGMP) apparaît.

Étape 3 Choisissez le numéro de version dans la liste déroulante Version.

Étape 4 Cliquez sur **OK**.

Configurer des fonctionnalités PIM

Les routeurs utilisent PIM pour gérer les tableaux de transfert à utiliser pour le transfert des diagrammes de multidiffusion. Lorsque vous activez le routage de multidiffusion sur ASA, PIM et IGMP sont automatiquement activés sur toutes les interfaces.



Remarque Le protocole PIM n'est pas pris en charge avec PAT. Le protocole PIM n'utilise pas de ports et PAT ne fonctionne qu'avec les protocoles qui utilisent des ports.

Cette section décrit comment configurer les paramètres PIM optionnels.

Activer et désactiver la PIM sur une interface

Vous pouvez activer ou désactiver la PIM sur des interfaces spécifiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface sur laquelle vous souhaitez activer la PIM dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit PIM Protocol** (Modifier le protocole PIM) apparaît.

Étape 3 Cochez la case **Enable PIM** (Activer la PIM). Pour désactiver la PIM, décochez cette case.

Étape 4 Cliquez sur **OK**.

Configurer une adresse de point de rendez-vous statique

Tous les routeurs d'un mode PIM fragmenté ou d'un domaine bidirectionnel commun doivent connaître l'adresse PRV PIM. L'adresse est configurée de manière statique à l'aide de la commande **pim rp-address**.

Remarque L'ASA ne prend pas en charge le PRV automatique.

Vous pouvez configurer l'ASA pour qu'il serve de PRV à plus d'un groupe. La plage de groupes spécifiée dans la liste de contrôle d'accès détermine le mappage du groupe RP PIM. Si aucune ACL n'est précisée, le RP du groupe est appliqué à l'ensemble de la plage du groupe de multidiffusion (224.0.0.0/4).

Procédure

Étape 1 Dans la fenêtre principale ASDM, choisissez**Configuration** > **Configuration du périphérique** > **Routage** > **Multidiffusion** > **PIM** > **Points de rendezvous**.

Étape 2 Cliquez sur **Add** ou **Edit** (Ajouter ou modifier).

La boîte de dialogue Add or Edit Rendezvous Point (Ajouter ou modifier un point de rendez-vous) s'affiche. La boîte de dialogue **Add Rendezvous Point** (Ajouter un point de rendez-vous) vous permet d'ajouter une nouvelle entrée au tableau des points de rendez-vous. La boîte de dialogue Edit Rendezvous Point (Modifier un point de rendez-vous) vous permet de modifier une entrée PRV existante. En outre, vous pouvez cliquer sur **Delete** (Supprimer) pour supprimer l'entrée du groupe de multidiffusion sélectionnée du tableau.

Ces restrictions s'appliquent aux PRV :

- Vous ne pouvez pas utiliser deux fois la même adresse RP.
- Vous ne pouvez pas spécifier Tous les groupes pour plus d'un RP.

Étape 3 Dans le champ **Rendezvous Point Address** (Adresse du point de rendez-vous), saisissez l'adresse IP du point de rendez-vous (PRV).

Lorsque vous modifiez une entrée PRV existante, vous ne pouvez pas modifier cette valeur.

Étape 4 Cochez la case **Use bi-directionnel forwarding** (Utiliser le transfert bidirectionnel) si les groupes de multidiffusion spécifiés doivent fonctionner en mode bidirectionnel. Le volet Rendezvous Point (Point de rendez-vous) affiche Yes (Oui) si les groupes de multidiffusion spécifiés doivent fonctionner en mode bidirectionnel et No (Non) si ces groupes doivent fonctionner en mode fragmenté. En mode bidirectionnel, si l'ASA reçoit un paquet en multidiffusion et n'a aucun membre connecté directement ou voisin PIM présent, il renvoie un message de suppression à la source.

Étape 5 Cliquez sur le bouton radio **Use this RP for All Multicast Groups** (Utiliser ce PRV pour tous les groupes de multidiffusion) pour utiliser le PRV spécifié pour tous les groupes de multidiffusion sur l'interface, ou sur le bouton radio **Use this RP for the Multicast Groups as specified below** (Utiliser ce PRV pour les groupes de multidiffusion spécifiés ci-dessous) pour désigner les groupes de multidiffusion à utiliser avec le PRV spécifié.

Pour en savoir plus sur les groupes de multidiffusion, consultez Configurer un groupe de multidiffusion, à la page 18.

Étape 6 Cliquez sur **OK**.

Configurer la priorité des routeurs désignés

Le DR est responsable de l'envoi des messages PIM de registre, de jonction et de suppression au RP. Lorsqu'il y a plusieurs routeurs de multidiffusion sur un segment de réseau, la sélection du DR se fait en fonction de la priorité DR. Si plusieurs périphériques ont le même DR, le périphérique avec l'adresse IP la plus élevée devient DR.

Par défaut, l'ASA a une priorité DR de 1. Vous pouvez modifier cette valeur.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez activer pour la PIM dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit PIM Protocol (Modifier le protocole PIM) apparaît.

Étape 3 Dans le champ DR Priority (Priorité DR), saisissez la valeur de la priorité de routeur désigné pour l'interface sélectionnée. Le routeur ayant la priorité DR la plus élevée sur le sous-réseau devient le routeur désigné. Les valeurs valides sont comprises entre 0 et 4294967294. La priorité DR par défaut est 1. Si cette valeur est fixée à 0, l'interface de l'ASA ne peut pas devenir le routeur par défaut.

Étape 4 Cliquez sur **OK**.

Configurer et filtrer les messages de registre PIM

Lorsque l'ASA agit comme un PRV, vous pouvez empêcher certaines sources en multidiffusion de s'enregistrer auprès de lui pour empêcher les sources non autorisées de s'enregistrer auprès du PRV. Le volet Request Filter (Filtre de demande) vous permet de définir les sources en multidiffusion dont l'ASA accepte les messages de registre PIM.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Request Filter (Filtre de demande)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue Request Filter Entry (Entrée du filtre de demande) vous permet de définir les sources de multidiffusion qui sont autorisées à s'enregistrer auprès de l'ASA lorsque celui-ci agit en tant que PRV. Vous créez les règles de filtre en fonction de l'adresse IP source et de l'adresse de multidiffusion de destination.

Étape 3 Dans la liste déroulante Action, sélectionnez Permet (Autoriser) pour créer une règle qui autorise la source spécifiée du trafic de multidiffusion spécifié à s'enregistrer auprès de l'ASA, ou sélectionnez Deny (Refuser)

pour créer une règle qui empêche la source spécifiée du trafic de multidiffusion spécifié de s'enregistrer auprès de l'ASA.

Étape 4 Saisissez l'adresse IP de la source du message de registre dans le champ Source IP Address (Adresse IP source).

Étape 5 Saisissez ou choisissez le masque réseau dans la liste déroulante de la source du message de registre, dans le champ Source Netmask (Masque réseau source).

Étape 6 Saisissez l'adresse de multidiffusion de destination dans le champ Destination IP Address (Adresse IP de destination).

Étape 7 Saisissez ou choisissez le masque réseau dans la liste déroulante de l'adresse de multidiffusion de destination, dans le champ Destination Netmask (Masque réseau de destination).

Étape 8 Cliquez sur **OK**.

Configurer les intervalles des messages PIM

Les messages de requête de routeur sont utilisés pour sélectionner le PIM DR. Le PIM DR est responsable de l'envoi des messages d'interrogation du routeur. Par défaut, des messages de requête du routeur sont envoyés toutes les 30 secondes. En outre, toutes les 60 secondes, l'ASA envoie des messages de jonction ou d'élimination PIM.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez activer pour la PIM dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit PIM Protocol (Modifier le protocole PIM) apparaît.

Étape 3 Saisissez la fréquence, en secondes, à laquelle l'interface envoie des messages Hello PIM, dans le champ Hello Interval (Intervalle Hello).

Étape 4 Saisissez la fréquence, en secondes, à laquelle l'interface envoie des annonces de jonction et d'élimination PIM, dans le champ Prune Interval (Intervalle d'élimination).

Étape 5 Cliquez sur **OK**.

Configurer une arborescence de routes

Par défaut, les routeurs secondaires PIM rejoignent l'arborescence du chemin le plus court immédiatement après l'arrivée du premier paquet en provenance d'une nouvelle source. Cette méthode réduit les délais, mais nécessite plus de mémoire que l'arborescence partagée. Vous pouvez configurer si l'ASA doit se joindre à l'arborescence du chemin le plus court ou utiliser l'arborescence partagée, soit pour tous les groupes de multidiffusion, soit uniquement pour des adresses de multidiffusion spécifiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Route Tree (Arborescence des routes)**.

Étape 2 Cliquez sur l'un des boutons radio suivants :

- **Use Shortest Path Tree for All Groups** (Utiliser l'arborescence du chemin le plus court pour tous les groupes) : choisissez cette option pour utiliser l'arborescence du chemin le plus court pour tous les groupes de multidiffusion.
- **Use Shared Tree for All Groups** (Utiliser l'arborescence partagée pour tous les groupes) pour utiliser l'arborescence partagée pour tous les groupes de multidiffusion.
- **Use Shared Tree for the Groups specified below** (Utiliser l'arborescence partagée pour les groupes spécifiés ci-dessous) : choisissez cette option pour utiliser l'arborescence partagée pour les groupes spécifiés dans le tableau des groupes de multidiffusion. L'arborescence du chemin le plus court est utilisée pour tout groupe qui n'est pas spécifié dans le tableau Groupes de multidiffusion.

  Le tableau Groupes de multidiffusion affiche les groupes de multidiffusion à utiliser avec l'arborescence partagée.

  Les entrées du tableau sont traitées de haut en bas. Vous pouvez créer une entrée qui comprend une plage de groupes de multidiffusion, mais exclut des groupes spécifiques de cette plage en mettant des règles de refus pour les groupes spécifiques en haut du tableau et la règle d'autorisation pour la plage de groupes en multidiffusion en dessous des instructions de refus.

  Pour modifier un groupe de multidiffusion, consultez Configurer un groupe de multidiffusion, à la page 18.

Configurer un groupe de multidiffusion

Les groupes de multidiffusion sont des listes de règles d'accès qui définissent les adresses de multidiffusion qui font partie d'un groupe. Un groupe de multidiffusion peut comprendre une adresse de multidiffusion unique ou une plage d'adresses de multidiffusion. Utilisez la boîte de dialogue Add Multidiffusion Group (Ajouter un groupe de multidiffusion) pour créer une nouvelle règle de groupe de multidiffusion. Utilisez la boîte de dialogue Edit Multicast Group (Modifier un groupe de multidiffusion) pour modifier une règle de groupe de multidiffusion existante.

Pour configurer un groupe de multidiffusion, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale ASDM, choisissez**Configuration** > **Configuration du périphérique** > **Routage** > **Multidiffusion** > **PIM** > **Points de rendezvous**.

Étape 2 Le volet Rendezvous Point s'affiche. Cliquez pour enregistrer le groupe que vous souhaitez configurer.

La boîte de dialogue Edit Rendezvous Point (Modifier le point de rendez-vous) s'affiche.

Étape 3 Cliquez sur le bouton d' **option Use this RP for the Multicast Groups comme précisé sous** le bouton radio pour désigner les groupes de multidiffusion à utiliser avec le RP précisé.

Étape 4 Cliquez sur **Add** ou **Edit**(ajouter ou modifier) .

La boîte de dialogue Add or Edit Multicast Group (ajouter ou modifier un groupe de multidiffusion) s'affiche.

Étape 5 Dans la liste déroulante Action (action), choisissez Allow pour créer une règle de groupe qui autorise les adresses de multidiffusion précisées ou choisissez Deny (refuser) pour créer une règle de groupe qui filtre les adresses de multidiffusion précisées.

Étape 6 Dans le champ Multicast Group Address (adresse de groupe de multidiffusion), saisissez l'adresse de multidiffusion associée au groupe.

Étape 7 Dans la liste déroulante Netmask, choisissez le masque de réseau pour l'adresse de groupe de multidiffusion.

Étape 8 Cliquez sur **OK**.

Filtrer les voisins PIM

Vous pouvez définir les routeurs qui peuvent devenir des voisins PIM. En filtrant les routeurs qui peuvent devenir des voisins PIM, vous pouvez effectuer les opérations suivantes :

- Empêchez les routeurs non autorisés de devenir des voisins PIM.
- Empêchez les routeurs tampons connectés de participer à PIM.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Neighbor Filter (Filtre de voisin)**.

Étape 2 Choisissez le voisin PIM que vous souhaitez configurer dans le tableau en cliquant sur **Add** (Ajouter)/**Edit** (Modifier)/**Insert** (Insérer).

La boîte de dialogue **Add/Edit/Insert Neighbor Filter Entry** (Ajouter/modifier/insérer une entrée de filtre de voisin) s'affiche. Elle vous permet de créer les entrées ACL pour la liste de contrôle d'accès de limite de multidiffusion. Vous pouvez également supprimer une entrée de voisin PIM sélectionnée.

Étape 3 Choisissez le nom de l'interface dans la liste déroulante **Interface Name** (Nom de l'interface).

Étape 4 Dans la liste déroulante **Action**, choisissez **Permit** (Autoriser) ou **Deny** (Refuser) pour l'entrée ACL du filtre de voisin.

Choisir Permit (Autoriser) permet aux annonces de groupes de multidiffusion de passer par l'interface. Si vous choisissez Deny (Refuser), les annonces de groupe de multidiffusion précisées ne passent pas par l'interface. Lorsqu'une limite de multidiffusion est configurée sur une interface, tout le trafic en multidiffusion ne peut pas passer par l'interface, à moins qu'une entrée de filtre de voisin ne le permette.

Étape 5 Saisissez l'adresse IP du groupe de PIM de multidiffusion autorisé ou refusé dans le champ **IP Address** (Adresse IP). Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.

Étape 6 Dans la liste déroulante **Netmask** (Masque réseau), choisissez le masque réseau pour l'adresse de groupe de multidiffusion.

Étape 7 Cliquez sur **OK**.

Configurer un filtre de voisin bidirectionnel PIM

Le volet Bidirectional Neighbor Filter (Filtre de voisin bidirectionnel) affiche les filtres de voisin bidirectionnel de la PIM, le cas échéant, qui sont configurés sur l'ASA. Un filtre de voisin bidirectionnel PIM est une ACL qui définit les périphériques voisins pouvant participer au choix du DF. Si un filtre de voisin bidirectionnel PIM n'est pas configuré pour une interface, il n'y a aucune restriction. Si un filtre de voisin bidirectionnel PIM est configuré, seuls les voisins autorisés par la liste de contrôle d'accès peuvent participer au processus de sélection de DF.

Lorsqu'une configuration de filtre de voisin bidirectionnel PIM est appliquée à l'ASA, une ACL s'affiche dans la configuration en cours d'exécution avec le nom *interface-name_multicast*, dans lequel le *interface-name* est le nom de l'interface à laquelle le filtre de limite de multidiffusion est appliqué. Si une ACL porte déjà ce nom, un numéro est affecté au nom (par exemple, inside_multicast_1). Cette ACL définit quels appareils peuvent devenir des voisins PIM de l'ASA.

Le PIM bidirectionnel permet aux routeurs de multidiffusion de conserver des informations d'état réduites. Tous les routeurs de multidiffusion d'un segment doivent être activés de manière bidirectionnelle pour choisir un DF.

Les filtres de voisin bidirectionnels de la PIM permettent la transition d'un réseau en mode fragmenté uniquement vers un réseau bidirectionnel en vous permettant de spécifier les routeurs qui doivent participer au choix du DF, tout en permettant à tous les routeurs de participer au domaine en mode fragmenté. Les routeurs bidirectionnels peuvent choisir un DF entre eux, même s'il y a des routeurs non-bidirectionnels sur le segment. La multidiffusion sur les routeurs non-bidirectionnels empêche les messages PIM et les données des groupes bidirectionnels de fuir vers l'intérieur ou l'extérieur du sous-ensemble bidirectionnel.

Lorsqu'un filtre de voisin bidirectionnel PIM est activé, les routeurs autorisés par la liste de contrôle d'accès sont considérés comme bidirectionnels. Par conséquent, ce qui suit est vrai :

- Si un voisin autorisé ne prend pas en charge le mode bidirectionnel, le choix du DF n'a pas lieu.
- Si un voisin refusé prend en charge le mode bidirectionnel, le choix du DF n'a pas lieu.
- Si un voisin refusé ne prend pas en charge le mode bidirectionnel, le choix du DF peut avoir lieu.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Bidirectional Neighbor Filter (Filtre de voisin bidirectionnel)**.

Étape 2 Cliquez deux fois sur une entrée dans le tableau des filtres de voisins bidirectionnels PIM pour accéder à la boîte de dialogue Edit Bidirectional Neighbor Filter Entry (Modifier une entrée de filtre de voisin bidirectionnel) pour cette entrée.

Étape 3 Choisissez le voisin PIM que vous souhaitez configurer dans le tableau en cliquant sur **Add** (Ajouter)/**Edit** (Modifier)/**Insert** (Insérer).

La boîte de dialogue **Add/Edit/Insert Bidirectional Neighbor Filter Entry (Ajouter/Modifier/Insérer une entrée de filtre de voisin bidirectionnel)** apparaît pour créer des entrées ACL pour l'ACL du filtre de voisin bidirectionnel PIM.

Étape 4 Choisissez le nom de l'interface dans la liste déroulante **Interface Name** (Nom de l'interface). Sélectionnez l'interface pour laquelle vous souhaitez configurer l'entrée ACL du filtre de voisin bidirectionnel PIM.

Étape 5 Dans la liste déroulante **Action**, choisissez **Permit** (Autoriser) ou **Deny** (Refuser) pour l'entrée ACL du filtre de voisin.

Choisissez Permit (Autoriser) pour autoriser les périphériques spécifiés à participer au processus de sélection du DF. Choisissez Deny (Refuser) pour empêcher les périphériques spécifiés de participer au processus de sélection du DF.

Étape 6 Saisissez l'adresse IP du groupe PIM de multidiffusion qui est autorisé ou refusé. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255, dans le champ IP Address (Adresse IP).

Étape 7 Dans la liste déroulante Netmask (Masque réseau), choisissez le masque réseau pour l'adresse de groupe de multidiffusion.

Étape 8 Cliquez sur **OK**.

Configurer l'ASA comme candidat BSR

Vous pouvez configurer l'ASA en tant que BSR candidat. Cela facilite également la découverte automatique du point de rendez-vous (PRV).

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Bootstrap Router (Routeur de démarrage)**.

Étape 2 Cochez la case **Configure this ASA as a candidate bootstrap router (CBSR)** (Configurer cet ASA en tant que routeur de démarrage candidat (CBSR)) pour effectuer la configuration de CBSR.

a) Dans la liste déroulante **Select Interface** (Sélectionner l'interface), sélectionnez l'interface sur l'ASA dont l'adresse BSR est dérivée pour en faire une interface candidate.



Remarque Cette interface doit être activée avec PIM.

b) Dans le champ **Hash mask length** (Longueur du masque de hachage), saisissez la longueur du masque (32 bits maximum) qui doit faire l'objet d'un AND avec l'adresse de groupe avant que la fonction de hachage ne soit appelée. Tous les groupes ayant le même hachage de départ correspondent au même point de rendez-vous (PRV). Par exemple, si cette valeur est 24, seuls les 24 premiers bits des adresses de groupe importent. Ce fait vous permet d'obtenir un RP pour plusieurs groupes.

c) Saisissez la priorité du BSR candidat dans le champ **Priority** (Priorité). Le BSR ayant la plus grande priorité est privilégié. Si les valeurs de priorité sont les mêmes, le routeur avec la plus grande adresse IP est le BSR. La valeur par défaut est 0.

Étape 3 (Facultatif) Sélectionnez une interface sur laquelle aucun message PIM BSR ne sera envoyé ou reçu dans la section **Configure this ASA as a Border Bootstrap Router** (Configurer cet ASA en tant que routeur de démarrage frontalier).

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer une limite de multidiffusion

La portée des adresses définit des limites de domaine afin que les domaines dont les RP ont la même adresse IP n'empiètent pas l'un sur l'autre. La détermination de la portée est effectuée sur les limites du sous-réseau au sein des grands domaines et sur les limites entre le domaine et Internet.

Vous pouvez configurer une limite de portée administrative sur une interface pour les adresses de groupe de multidiffusion. L'IANA a désigné la plage d'adresses en multidiffusion de 239.0.0.0 à 239.255.255.255 comme adresses de portée administrative. Cette plage d'adresses peut être réutilisée dans des domaines administrés par différentes organisations. Les adresses seraient considérées comme locales et non uniques mondialement.

Une liste de contrôle d'accès standard définit la plage d'adresses concernées. Lorsqu'une limite est configurée, aucun paquet de données en multidiffusion ne peut traverser la limite dans aucune direction. La limite permet à la même adresse de groupe de multidiffusion d'être réutilisée dans différents domaines administratifs.

Vous pouvez configurer, examiner et filtrer les messages de découverte et d'annonce Auto-RP à la limite administrative. Toutes les annonces de plage de groupes Auto-RP des paquets Auto-RP qui sont refusées par l'ACL de frontière sont supprimées. Une annonce de plage de groupes Auto-RP est autorisée et transmise par la limite uniquement si toutes les adresses de la plage de groupes Auto-RP sont autorisées par la liste de contrôle d'accès (ACL) de limite. Si une adresse n'est pas autorisée, la plage complète de groupe est filtrée et supprimée du message Auto-RP avant que le message Auto-RP ne soit transféré.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **MBoundary (Limite de multidiffusion)**.

Le volet MBoundary (Limite de multidiffusion) vous permet de configurer une limite de multidiffusion pour les adresses de multidiffusion de portée administrative. Une limite de multidiffusion restreint les flux de paquets de données en multidiffusion et permet la réutilisation de la même adresse de groupe de multidiffusion dans différents domaines administratifs. Lorsqu'une limite de multidiffusion est définie sur une interface, seul le trafic en multidiffusion autorisé par la liste de contrôle d'accès du filtre passe par l'interface.

Étape 2 Cliquez sur **Edit**.

La boîte de dialogue Edit Boundary Filter (Modifier le filtre de limite) apparaît et affiche l'ACL du filtre de limite de multidiffusion. Vous pouvez ajouter et supprimer des entrées d'ACL de filtre de limite à l'aide de cette boîte de dialogue.

Lorsque la configuration du filtre de limite est appliquée à l'ASA, l'ACL apparaît dans la configuration d'exécution avec le nom *interface-name*_multicast, où *interface-name* est le nom de l'interface à laquelle le filtre de limite de multidiffusion est appliqué. Si une ACL porte déjà ce nom, un numéro est affecté au nom (par exemple, inside_multicast_1).

Étape 3 Dans la liste déroulante Interface, choisissez l'interface pour laquelle vous configurez l'ACL du filtre de limite de multidiffusion.

Étape 4 Cochez la case **Remove any Auto-RP group range** (Supprimer toute plage de groupes Auto-RP) pour filtrer les messages Auto-RP des sources refusées par l'ACL de la limite. Si la case **Remove any Auto-RP group range** (Supprimer toute plage de groupes Auto-RP) n'est pas cochée, tous les messages Auto-RP sont transmis.

Étape 5 Cliquez sur **OK**.

Supervision de PIM

Pour superviser ou désactiver diverses statistiques de routage PIM, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **BSR Router (Routeur BSR)**

Les renseignements relatifs à la configuration du routeur BSR s'affichent.

Étape 2 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **Multicast Routing Table (Table de routage de multidiffusion)**

Le contenu de la table de routage de multidiffusion s'affiche.

Étape 3 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **MFIB**

Les renseignements récapitulatifs sur le nombre d'entrées et d'interfaces de la base d'information de transfert multidiffusion PIM IPv4 s'affichent.

Étape 4 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **MFIB Active (MFIB active)**

Les renseignements récapitulatifs de la base d'information de transfert multidiffusion (MFIB) sur le débit auquel les sources de multidiffusion actives envoient des données aux groupes de multidiffusion s'affichent.

Étape 5 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **Group Map (Mappage de groupe)**

Les renseignements récapitulatifs de la base d'information de transfert multidiffusion (MFIB) sur le débit auquel les sources de multidiffusion actives envoient des données aux groupes de multidiffusion s'affichent.

a) Sélectionnez **RP Timers** (Minuteries RP) dans la liste déroulante **Select PIM Group** (Sélectionner un groupe PIM), pour afficher les renseignements sur la minuterie pour chaque mappage de groupe vers le mode PIM.

Étape 6 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **Neighbors (Voisins)**

Les renseignements sur le voisin PIM (Protocole Independent Multicast) s'affichent.

Exemple de routage de multidiffusion

L'exemple suivant montre comment activer et configurer le routage de multidiffusion à l'aide de différents processus facultatifs :

1. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)**.

2. Dans le volet Multicast (Multidiffusion), cochez la case **Enable Multicast routing** (Activer le routage de multidiffusion), puis cliquez sur **Apply** (Appliquer).
3. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **MRoute**.
4. Cliquez sur **Add** ou **Edit** (Ajouter ou modifier) .

   La boîte de dialogue Add or Edit Multicast Route (Ajouter ou modifier une route de multidiffusion) s'affiche.

   Utilisez la boîte de dialogue Add Multicast Route (Ajouter une route de multidiffusion) pour ajouter une nouvelle route de multidiffusion statique à l'ASA. Utilisez la boîte de dialogue Edit Multicast Route (Modifier une route de multidiffusion) pour modifier une route de multidiffusion statique existante.
5. Dans le champ Source Address (Adresse source), saisissez l'adresse IP de la source de multidiffusion. Vous ne pouvez pas modifier cette valeur lors de la modification d'une route de multidiffusion statique existante.
6. Choisissez le masque réseau pour l'adresse IP de la source de multidiffusion dans la liste déroulante Source Mask (Masque source).
7. Dans la zone Incoming Interface (Interface entrante), cliquez sur le bouton radio **RPF Interface** (Interface RPF) pour choisir RPF pour transférer le routage ou sur le bouton radio **Interface Name** (Nom de l'interface), puis saisissez la commande suivante :
   - Dans le champ Source Interface (Interface source), choisissez l'interface entrante pour la route de multidiffusion dans la liste déroulante.
   - Dans le champ Destination Interface (Interface de destination), choisissez l'interface de destination à laquelle la route est transférée par l'intermédiaire de l'interface sélectionnée dans la liste déroulante.

Remarque Vous pouvez spécifier l'interface ou le voisin RPF, mais pas les deux en même temps.

8. Dans le champ Administrative Distance (Distance administrative), choisissez la distance administrative de la route de multidiffusion statique. Si la route de multidiffusion statique a la même distance administrative que la route de monodiffusion, la route de multidiffusion statique prévaut.
9. Cliquez sur **OK**.
10. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Join Group (Groupe de jonction)**.

    Le volet Join Group (Groupe de jonction) apparaît.
11. Cliquez sur **Add** ou **Edit** (Ajouter ou modifier).

    La boîte de dialogue Add IGMP Join Group (Ajouter un groupe de jonction IGMP) vous permet de configurer une interface pour qu'elle soit membre d'un groupe de multidiffusion. La boîte de dialogue Edit IGMP Join Group (Modifier un groupe de jonction IGMP) vous permet de modifier les renseignements d'appartenance existants.

12. Dans le champ Interface Name (Nom de l'interface), choisissez le nom de l'interface dans la liste déroulante. Si vous modifiez une entrée existante, vous ne pouvez pas modifier cette valeur.
13. Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse d'un groupe de multidiffusion auquel appartient l'interface. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.
14. Cliquez sur **OK**.

Historique du routage de multidiffusion

Tableau 2 : Historique des fonctionnalités du routage de multidiffusion

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage de multidiffusion sur un tunnel de l'interface de tunnel virtuel statique	9.24(10)	Vous pouvez fournir en toute sécurité des applications de multidiffusion en temps réel, telles que la diffusion en flux continu de vidéos, les flux de données financières et la réplication de données sur votre infrastructure VPN en utilisant des tunnels IPsec configurés avec un VTI statique.
Prise en charge du routage de multidiffusion	7.0(1)	La prise en charge des données de routage de multidiffusion, de l'authentification, de la redistribution et de la surveillance des informations de routage à l'aide du protocole de routage de multidiffusion a été ajoutée. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Multicast (Multidiffusion).
Prise en charge de la mise en grappe	9.0(1)	Une prise en charge a été ajoutée pour la mise en grappe.
Prise en charge du protocole PIM (Protocol Independent Multicast) en multidiffusion propre à la source (PIM-SSM)	9.5(1)	Une prise en charge a été ajoutée pour permettre aux paquets PIM-SSM de transiter lorsque le routage de multidiffusion est activé, sauf si l'ASA est le routeur de dernier saut. Cela permet une plus grande flexibilité dans le choix d'un groupe de multidiffusion tout en vous assurant une protection contre différentes attaques; les hôtes ne reçoivent que le trafic de sources explicitement demandées. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routeur de démarrage PIM (Protocol Independent Multicast)	9.5(2)	Une prise en charge a été ajoutée pour un nouveau modèle de sélection dynamique des points de rendez-vous (PRV) qui utilise des routeurs candidats pour la fonction Point de rendez-vous et pour le relais des informations Point de rendez-vous pour un groupe. Cette fonctionnalité fournit un moyen d'apprendre dynamiquement les points de rendez-vous (PRV), ce qui est tout à fait essentiel dans les grands réseaux complexes où un PRV peut périodiquement tomber en panne et se relancer. Nous avons introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Multicast (Multidiffusion) > PIM > Bootstrap Router (Routeur de démarrage)
Limite igmp augmentée	9.15(1) *Également dans 9.12(4)*	La limite igmp a été augmentée de 500 à 5 000. Nous n'avons pas modifié d'écrans.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.