Routage multidiffusion

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

À propos du routage de 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 qui tirent parti du routage de multidiffusion comprennent les vidéoconférences, les communications d'entreprise, l'apprentissage à distance et la distribution de logiciels, de cotations boursières et d'actualités.

Les protocoles de routage de multidiffusion acheminent le trafic source vers plusieurs récepteurs sans ajouter de charge supplémentaire pour la source ou les récepteurs, tout en utilisant la moindre bande passante de réseau de toutes les technologies concurrentes. Les paquets en multidiffusion sont répliqués dans le réseau par l'activation de 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 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. Vous devez activer PIM sur les interfaces qui participent au routage de la 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 enracinées à un seul point RP (Rendez-vous point) par groupe de multidiffusion et crée éventuellement des arborescences du chemin le plus court par 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. 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, sans nécessiter d'état propre 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 du ASA comme adresse RP.

Prise en charge de la multidiffusion PIM propre à la source

L'ASA ne prend pas en charge la fonctionnalité PIM de multidiffusion source spécifique (SSM) et la configuration associée. Cependant, l'ASA permet aux paquets liés au SSM de passer, sauf s'il est placé comme routeur de dernier saut.

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.

PIM-SSM diffère de PIM-SM en ce qu'il n'utilise pas de RP ou d'arborescence partagée. Au lieu de cela, les informations sur les adresses de sources d'un groupe de multidiffusion sont fournies par les récepteurs au moyen du protocole IGMPv3) et sont utilisées pour créer directement des arborescences propres aux sources.

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 fournit un moyen d'apprendre dynamiquement les RP, ce qui est tout à fait essentiel dans les grands réseaux complexes où un RP peut périodiquement tomber en panne et se relancer.

Terminologie du routeur de démarrage PIM (BSR)

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'issu 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 frontière physique ou géographique : les hôtes peuvent être situés n'importe où sur Internet. Les hôtes qui souhaitent recevoir des données vers un groupe en particulier doivent rejoindre ce groupe au moyen d'IGMP. Les hôtes doivent être membres du groupe pour recevoir le flux de données.

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

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

Ne prend pas en charge IPv6.

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. Par conséquent, le routage de multidiffusion Internet à partir de la plage d'adresses 224.0.0/24 n'est pas pris en charge; Le groupe IGMP n'est pas créé lors de l'activation du routage de multidiffusion pour les adresses réservées.

Mise en grappe

En grappe, pour IGMP et PIM, cette fonctionnalité n'est prise en charge que sur l'unité principale.

Directives supplémentaires

- 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.
- Le routage de multidiffusion PIM/IGMP n'est pas pris en charge sur les interfaces dans une zone de trafic.
- 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 RP est acheminée par l'intermédiaire d'une adresse IP de secours HSRP, le routage de multidiffusion ne fonctionne pas dans ASA. Par conséquent, pour que le trafic en multidiffusion réussisse, assurez-vous que la voie de routage pour l'adresse RP n'est pas l'adresse IP de secours HSRP. Configurez plutôt l'adresse de routage sur une adresse IP d'interface.

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

Activez le routage de multidiffusion :

multicast-routing

Exemple :

```
ciscoasa(config)# multicast-routing
```

Le nombre d'entrées dans les tables de routage de multidiffusion est limité par la quantité de RAM sur l'ASA.

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

Configurez le routage de multidiffusion de stub et transférez les messages IGMP :

igmp forward interface if_name

Exemple :

```
ciscoasa(config-if)# igmp forward interface interface1
```

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 Configurez une route de multidiffusion statique :

mroute src_ip src_mask {input_if_name | *rpf_neighbor*} [distance]

Exemple :

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
```

Étape 2 Configurez une route de multidiffusion statique pour une zone de stub :

mroute src_ip src_mask input_if_name [**dense** output_if_name] [distance]

Exemple :

```
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

Le paire mot clé-argument **dense** *output_if_name* n'est prise en charge que pour le routage de multidiffusion de stub.

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

Désactivez IGMP sur une interface :

no igmp

Exemple :

```
ciscoasa(config-if)# no igmp
```

Pour réactiver IGMP sur une interface, utilisez la commande **igmp**.

Remarque
Seule la commande **no igmp** apparaît dans la configuration d'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 8.

Procédure

Configurez l'ASA pour qu'il soit membre d'un groupe de multidiffusion :

igmp join-group group-address

Exemple :

```
ciscoasa(config-if)# igmp join-group mcast-group
```

L'argument *group-address* est l'adresse IP du groupe.

Remarque
La commande **igmp join-group** permet à PIM d'envoyer des demandes de *jonction* vers les sources ou vers le point de rendez-vous (RP), à condition que le pare-feu avec cette commande soit le routeur désigné PIM (DR) sur l'interface où la commande est appliquée.

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.

Entrez la commande **igmp static-group**. L'ASA n'accepte pas les paquets de multidiffusion, mais les transfère plutôt vers l'interface spécifiée.

Procédure

Configurez l'ASA de manière statique pour qu'il rejoigne un groupe de multidiffusion sur une interface :

igmp static-group

Exemple :

```
ciscoasa(config-if)# igmp static-group group-address
```

L'argument *group-address* est l'adresse IP du groupe.

Remarque
La commande **igmp static-group** permet à PIM d'envoyer des demandes de *jonction* vers les sources ou vers le point de rendez-vous (RP), à condition que le pare-feu avec cette commande soit le routeur désigné PIM (DR) sur l'interface où la commande est appliquée.

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 Créez une ACL standard pour le trafic de multidiffusion :

access-list name **standard** [**permit | deny]** ip_addr mask

Exemple :

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

Vous pouvez créer plusieurs entrées pour une seule ACL. Vous pouvez utiliser des ACL étendues ou standard.

L'argument *ip_addr mask* est l'adresse IP du groupe de multidiffusion qui est autorisée ou refusée.

Étape 2 Créez une ACL étendue :

access-list name **extended** [**permit | deny]** protocol src_ip_addr src_mask dst_ip_addr dst_mask

Exemple :

```
ciscoasa(config)# access-list acl2 extended permit protocol
src_ip_addr src_mask dst_ip_addr dst_mask
```

L'argument *dst_ip_addr* est l'adresse IP du groupe de multidiffusion qui est autorisée ou refusée.

Étape 3 Appliquez l'ACL à une interface :

igmp access-group acl

Exemple :

```
ciscoasa(config-if)# igmp access-group acl
```

L'argument *acl* est le nom d'une ACL IP standard ou étendue.

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

Limitez le nombre d'états IGMP sur une interface :

igmp limit number

Exemple :

```
ciscoasa(config-if)# igmp limit 50
```

Les valeurs valides sont comprises entre 0 et 5 000, étant la valeur par défaut.

La définition de cette valeur à 0 empêche l'ajout de groupes appris, mais les appartenances définies manuellement (à l'aide des commandes **igmp join-group** et **igmp static-group**) sont toujours autorisées. La forme **no** (non) de cette commande rétablit la valeur par défaut.

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.

Remarque Les commandes **igmp query-timeout** et **igmp query-interval** nécessitent IGMP version 2.

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 Définissez la durée de l'intervalle de requête en secondes :

igmp query-interval *seconds*

Exemple :

```
ciscoasa(config-if)# igmp query-interval 30
```

Les valeurs valides vont de 1 à 3600; la valeur par défaut est 125.

Si l'ASA n'entend pas de message de requête sur une interface pendant le délai d'expiration spécifié (255 secondes par défaut), l'ASA devient le routeur désigné et commence à envoyer les messages de requête.

Étape 2 Modifiez la valeur du délai d'expiration de la requête :

igmp query-timeout *seconds*

Exemple :

```
ciscoasa(config-if)# igmp query-timeout 30
```

Les valeurs valides vont de 60 à 300; la valeur par défaut est 225.

Étape 3 Modifiez le temps de réponse maximum aux requêtes :

igmp query-max-response-time *seconds*

Les valeurs valides vont de 1 à 25; la valeur par défaut est 10.

Exemple :

```
ciscoasa(config-if)# igmp query-max-response-time 20
```

Modifier la version IGMP

Par défaut, l'ASA exécute la version 2 du protocole IGMP, qui active plusieurs fonctionnalités supplémentaires telles que les commandes **igmp query-timeout** et **igmp query-interval** .

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

Contrôlez la version d'IGMP que vous souhaitez exécuter sur l'interface :

igmp version {**1** | **2**}

Exemple :

```
ciscoasa(config-if)# igmp version 2
```

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 Activez ou réactivez la PIM sur une interface spécifique :

pim

Exemple :

```
ciscoasa(config-if)# pim
```

Étape 2 Désactivez la PIM sur une interface spécifique :

no pim

Exemple :

```
ciscoasa(config-if)# no pim
```

Remarque
Seule la commande **no pim** apparaît dans la configuration d'interface.

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 devez utiliser la commande **pim rp-address** pour spécifier l'adresse PRV.

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

Activez ou réactivez la PIM sur une interface spécifique :

pim rp-address ip_address [acl] [**bidir**]

L'argument *ip_address* est l'adresse IP de monodiffusion du routeur attribué comme PRV PIM.

L'argument *acl* est le nom ou le numéro d'une ACL standard qui définit avec quels groupes de multidiffusion le PRV doit être utilisé. N'utilisez pas une ACL d'hôte avec cette commande.

L'exclusion du mot clé **bidir** fait que les groupes fonctionnent en mode PIM fragmenté.

Remarque
L'ASA annonce toujours la capacité bidirectionnelle dans les messages Hello de PIM, quelle que soit la configuration bidirectionnel réelle.

Exemple :

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

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

Changez la priorité du routeur désigné :

pim dr-priority num

Exemple :

```
ciscoasa(config-if)# pim dr-priority 500
```

L'argument *num* peut être n'importe quel nombre compris entre 1 et 4294967294.

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

Configurez l'ASA pour filtrer les messages de registre PIM :

pim accept-register {**list** acl | **route-map** map-name}

Exemple :

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

Dans l'exemple, l'ASA filtre les messages de registre PIM *acl1* et de carte de routage *map2*.

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 Envoyez les messages de requête du routeur :

pim hello-interval seconds

Exemple :

```
ciscoasa(config-if)# pim hello-interval 60
```

Les valeurs valides pour l'argument *seconds* sont comprises entre 1 et 3 600 secondes.

Étape 2 Modifiez la durée (en secondes) pendant laquelle l'ASA envoie des messages de jonction ou d'élimination PIM :

pim join-prune-interval seconds

Exemple :

```
ciscoasa(config-if)# pim join-prune-interval 60
```

Les valeurs valides pour l'argument *seconds* sont comprises entre 10 et 600 secondes.

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 Utilisez une ACL standard pour définir les routeurs que vous souhaitez voir participer à la PIM :

access-list pim_nbr deny *router-IP_addr PIM neighbor*

Exemple :

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

Dans l'exemple, l'ACL suivante, lorsqu'elle est utilisée avec la commande **pim neighbor-filter**, empêche le routeur 10.1.1.1 de devenir un voisin PIM.

Étape 2 Filtrez les routeurs voisins :

pim neighbor-filter pim_nbr

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

Dans l'exemple, le routeur 10.1.1.1 ne peut pas devenir un voisin PIM sur l'interface GigabitEthernet0/3.

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 Utilisez une ACL standard pour définir les routeurs que vous souhaitez voir participer à la PIM :

access-list pim_nbr deny *router-IP_addr PIM neighbor*

Exemple :

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

Dans l'exemple, l'ACL suivante, lorsqu'elle est utilisée avec la commande **pim neighbor-filter**, empêche le routeur 10.1.1.1 de devenir un voisin PIM.

Étape 2 Filtrez les routeurs voisins :

pim bidirectional-neighbor-filter pim_nbr

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

Dans l'exemple, le routeur 10.1.1.1 ne peut pas devenir un voisin bidirectionnel PIM sur l'interface GigabitEthernet0/3.

Configurer l'ASA comme candidat BSR

Vous pouvez configurer l'ASA en tant que BSR candidat.

Procédure

Étape 1 Configurez le routeur pour qu'il annonce sa candidature en tant que routeur de démarrage (BSR) :

pim bsr-candidate *interface_name* [*hash_mask_length* [*priority*]]

Exemple :

```
ciscoasa(config)# pim bsr-candidate inside 12 3
```

Étape 2 (Facultatif) Configurez l'ASA en tant que routeur de démarrage frontalier :

interface *interface_name*

pim bsr-border

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# pim bsr-border
```

Lorsque cette commande est configurée sur une interface, aucun message de routeur de démarrage (BSR) ne sera envoyé ou reçu par le biais d'une interface.

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 en saisissant le mot clé **filter-autorp**. 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

Configurez une limite de multidiffusion :

multicast boundary acl [**`filter-autorp`**]

Exemple :

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

Supervision de PIM

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage PIM. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande.

Pour superviser ou désactiver diverses statistiques de routage PIM, saisissez l'une des commandes suivantes :

- **show pim bsr-router**

  Affiche les renseignements sur le routeur de démarrage.

- **show mroute**

  Affiche le contenu de la table de routage multidiffusion.

- **show mfib summary**

Affiche des renseignements récapitulatifs sur le nombre d'entrées et d'interfaces de la base d'information de transfert multidiffusion PIM IPv4.

- **show mfib active**

  Affiche les renseignements 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.

- **show pim group-map**

  Affiche le mappage de groupe vers le mode PIM. Pour afficher le RP choisi pour un groupe, précisez l'adresse ou le nom du groupe.

- **show pim group-map rp-timers**

  Affiche l'expiration et le temps de disponibilité de la minuterie pour chaque entrée de mappage de groupe vers le mode PIM.

- **show pim neighbor**

  Affiche les voisins PIM (Protocole Independent Multicast).

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. Activez le routage de multidiffusion :

   ```
   ciscoasa(config)# multicast-routing
   ```

2. Configurez une route de multidiffusion statique :

   ```
   ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
   ciscoasa(config)# exit
   ```

3. Configurez l'ASA pour qu'il soit membre d'un groupe de multidiffusion :

   ```
   ciscoasa(config)# interface
   ciscoasa(config-if)# igmp join-group group-address
   ```

Historique du routage de multidiffusion

Tableau 1 : Historique des fonctionnalités du routage de multidiffusion

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
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 la commande **multicast-routing**.
Prise en charge de la mise en grappe	9.0(1)	Une prise en charge a été ajoutée pour la mise en grappe. Nous avons introduit les commandes suivantes : **debug mfib cluster**, **show mfib cluster**.
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 de commandes.
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 ajouté les commandes suivantes : clear pim group-map, debug pim bsr, pim bsr-border, pim bsr-candidate, show pim bsr-router, show pim group-map rp-timers
Limite igmp augmentée	9.15(1) *Également dans 9.12(4)*	La limite igmp a été augmentée de 500 à 5 000. Commandes nouvelles ou modifiées : **igmp limit**.

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.