Multicast (multidiffusion)

Ce chapitre décrit comment configurer Appareil Cisco Secure Firewall Threat Defense 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 appareil de défense contre les menaces 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'appareil de défense contre les menaces 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 appareil de défense contre les menaces .

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.

Protocole IGMP

Les hôtes IP utilisent le protocole IGMP (Internet Group Management Protocol) 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.

IGMP utilise des adresses de groupe (adresse IP de classe D) comme identifiants de groupe. L'adresse de groupe d'hôtes peut être comprise entre 224.0.0.0 et 239.255.255.255. L'adresse 224.0.0.0 n'est jamais attribuée à un groupe. L'adresse 224.0.0.1 est attribuée à tous les systèmes d'un sous-réseau. L'adresse 224.0.0.2 est attribuée à tous les routeurs d'un sous-réseau.

Remarque Lorsque vous activez le routage de multidiffusion sur le périphérique défense contre les menaces , le protocole IGMP version 2 est automatiquement activé sur toutes les interfaces.

Interroger les messages destinés aux groupes de multidiffusion

Le périphérique défense contre les menaces 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 informations sur les membres stockées sur le périphérique défense contre les menaces . Si le périphérique défense contre les menaces découvre qu'il n'y a aucun membre local d'un groupe de multidiffusion connecté à une interface, il arrête de transférer les paquets 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 le périphérique défense contre les menaces ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.

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'appareil de défense contre les menaces agit comme un agent mandataire IGMP. Au lieu de participer entièrement au routage de multidiffusion, l'appareil de défense contre les menaces 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'appareil de défense contre les menaces 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'appareil de défense contre les menaces 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 appareil de défense contre les menaces est le RP du PIM, utilisez l'adresse externe non traduite du appareil de défense contre les menaces comme adresse RP.

Prise en charge de la multidiffusion PIM propre à la source

L'appareil de défense contre les menaces ne prend pas en charge la fonctionnalité PIM de multidiffusion source spécifique (SSM) et la configuration associée. Cependant, l'appareil de défense contre les menaces 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.

Multidiffusion bidirectionnelle PIM

La PIM bidirectionnelle en multidiffusion est utile pour les réseaux dans lesquels de nombreuses sources et récepteurs communiquent simultanément et où chaque participant peut devenir à la fois la source et le récepteur du trafic en multidiffusion, comme lors de vidéoconférences, de réunions Webex et de clavardages de groupe. Lorsque le mode bidirectionnel PIM est utilisé, le RP crée uniquement l'entrée (*,G) pour l'arborescence partagée. Il n'y a pas d'entrée (S, G). Cela permet d'économiser les ressources sur le RP, car les tableaux d'états de chaque entrée (S,G) ne sont pas conservés.

En mode PIM dispersé, le trafic ne circule que dans l'arborescence partagée. En mode PIM bidirectionnel, le trafic circule de haut en bas dans l'arborescence partagée.

Le mode bidirectionnel PIM n'utilise pas non plus le mécanisme d'enregistrement/arrêt d'enregistrement PIM pour enregistrer les sources sur le RP. Chaque source peut commencer à envoyer à la source à tout moment.

Lorsque les paquets en multidiffusion arrivent au RP, ils sont acheminés vers le bas de l'arborescence partagée (s'il y a des récepteurs) ou abandonnés (en l'absence de récepteur). Cependant, il n'y a aucun moyen pour le RP de dire à la source d'arrêter d'envoyer le trafic en multidiffusion.

Du point de vue de la conception, vous devez penser à l'endroit où placer le RP dans votre réseau, car il devrait être quelque part au milieu entre les sources et les récepteurs du réseau.

Le mode PIM bidirectionnel n'a aucune vérification du transfert de chemin inverse (reversed path forwarding ou RPF). Au lieu de cela, il utilise le concept de transitaire désigné (DF) pour éviter les boucles. Cette DF est le seul routeur du segment à être autorisé à envoyer du trafic en multidiffusion vers le RP. S'il n'y a qu'un seul routeur par segment qui transmet le trafic en multidiffusion, il n'y aura pas de boucle. Le DF est choisi au moyen du mécanisme suivant :

- Le routeur avec la mesure la plus basse pour le RP est le DF.
- Si la métrique est égale, le routeur avec l'adresse IP la plus élevée devient le DF.

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'appareil de défense contre les menaces 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 grappes

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.

Exigences et conditions préalables au routage de multidiffusion

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices pour le routage de multidiffusion

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 grappes

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

Directives supplémentaires

- Vous devez configurer un contrôle d’accès ou une règle de préfiltre sur la zone de sécurité entrante pour autoriser le trafic vers l’hôte de multidiffusion, tel que la zone 224.1.2.3. Cependant, vous ne pouvez pas spécifier de zone de sécurité de destination pour la règle, ou elle ne peut pas être appliquée aux connexions en multidiffusion lors de la validation initiale de la connexion.
- Vous ne pouvez pas désactiver une interface pour laquelle un PIM est configuré. Si vous avez configuré PIM sur l’interface (voir Configurer le protocole PIM, à la page 12), la désactivation du routage de multidiffusion et de PIM ne supprime pas la configuration PIM. Vous devez retirer (supprimer) la configuration PIM pour désactiver l’interface.
- Le routage de multidiffusion PIM/IGMP n’est pas pris en charge sur les interfaces dans une zone de trafic.
- Ne configurez pas défense contre les menaces 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 défense contre les menaces. 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.

- Pour un périphérique utilisant le routage virtuel, vous pouvez configurer la multidiffusion uniquement pour son routeur virtuel global et non pour son routeur virtuel défini par l'utilisateur.

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.

Procédure

Étape 1 Routage multidiffusion activé, à la page 7.
Étape 2 Configurer le protocole IGMP, à la page 8.
Étape 3 Configurer des groupes d'accès IGMP, à la page 9.
Étape 4 Configurer des groupes statiques IGMP, à la page 10.
Étape 5 Configurer des groupes de jonction IGMP, à la page 11.

Routage multidiffusion activé

L'activation du routage de multidiffusion sur le périphérique défense contre les menaces active par défaut IGMP et PIM sur toutes les interfaces. 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.

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 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing** > **Multicast Routing (routage de multidiffusion) >IGMP** ».

Étape 3 Cochez la case **Enable Multicast Routing** (activer le routage de multidiffusion).

Cochez cette case pour activer le routage de multidiffusion IP sur le périphérique. 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. Cela est utile si vous savez qu'il n'y a aucun hôte en multidiffusion sur une interface spécifique et que vous souhaitez empêcher le périphérique défense contre les menaces d'envoyer des messages de requête d'hôte sur cette interface.

Configurer le protocole IGMP

Vous pouvez configurer les paramètres IGMP par interface, comme l'interface de transfert, les messages de requête et les intervalles temporels.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **IGMP (IGMP)**.

Étape 3 Dans le menu **Protocol** (protocole), cliquez sur **Add** (ajouter) ou **Edit** (modifier).

Utilisez la boîte de dialogue **Add IGMP settings** (ajouter des paramètres IGMP) pour ajouter de nouveaux paramètres IGMP au périphérique défense contre les menaces . Utilisez la boîte de dialogue **Edit IGMP settings** (modifier les paramètres IGMP) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- **Interface** : dans la liste déroulante, choisissez l'interface pour laquelle vous souhaitez configurer le protocole IGMP.
- **Enable IGMP** : cochez la case pour activer IGMP.

  Remarque La désactivation de IGMP sur des interfaces spécifiques est utile si vous savez qu'il n'y a aucun hôte de multidiffusion sur une interface spécifique et que vous souhaitez empêcher le périphérique d'envoyer des messages de requête d'hôte sur cette interface.

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

  Cela configure le périphérique Cisco Secure Firewall Threat Defense 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.

- **Version** : choisissez IGMP Version 1 ou 2.

  Par défaut, le périphérique défense contre les menaces exécute la version 2 du protocole IGMP, qui active plusieurs fonctionnalités supplémentaires.

  Remarque Tous les routeurs de multidiffusion d'un sous-réseau doivent prendre en charge la même version d'IGMP. Le périphérique défense contre les menaces ne détecte pas automatiquement les routeurs de la version 1 et passe à la version 1. Cependant, vous pouvez avoir une combinaison d'hôtes IGMP versions 1 et 2 sur le sous-réseau; le périphérique défense contre les menaces exécutant IGMP version 2 fonctionne correctement lorsque des hôtes IGMP version 1 sont présents.

- **Query Interval** (intervalle de requête) : intervalle en secondes auquel le routeur désigné envoie des messages de requête d'hôte IGMP. La plage est comprise entre 1 et 3600. La valeur par défaut est 125.

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

- **Response Time** (Temps de réponse) : l'intervalle en secondes avant que le périphérique défense contre les menaces ne supprime le groupe. La plage est de 1 à 25. La valeur par défaut est 10.

  Si le périphérique défense contre les menaces ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.

- **Group Limit** (limite de groupe) : le nombre maximal d'hôtes qui peuvent rejoindre une interface. La valeur doit être comprise entre 1 et 500. La valeur par défaut est 500.

  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.

- **Query Timeout**(délai d'expiration de la requête) : la période en secondes avant laquelle le périphérique défense contre les menaces prend le relais en tant que demandeur pour l'interface après l'arrêt du demandeur précédent. La valeur doit être comprise entre 60 et 300. La valeur par défaut est 255.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du protocole IGPM.

Configurer des groupes d'accès IGMP

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

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routage** > **Routage de multidiffusion** > **Groupe d'accès**.

Étape 3 Dans **Groupe d'accès**, cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add IGMP Access Group parameters** (Ajouter les paramètres du groupe d'accès IGMP) pour ajouter de nouveaux groupes d'accès IGMP au tableau Access Group (groupes d'accès). Utilisez

la boîte de dialogue **Edit IGMP Access Group parameters** (Ajouter les paramètres du groupe d'accès IGMP) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

a) Dans la liste déroulante **Interface**, choisissez l'interface à laquelle le groupe d'accès est associé. Vous ne pouvez pas modifier l'interface associée lorsque vous modifiez un groupe d'accès existant.

b) Cliquez sur l'un des éléments suivants :

- **Standard Access List**(liste d'accès standard) : dans la liste déroulante **Standard Access List**, sélectionnez la liste de contrôle d'accès standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard pour connaître la procédure.
- **Extended Access List**(liste d'accès étendue) : dans la liste déroulante **Extended Access List**, sélectionnez la liste d'accès étendue ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL étendue. Reportez-vous à Configurer les objets ACL étendus pour connaître la procédure.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du groupe statique.

Configurer des groupes statiques IGMP

Parfois, un membre d'un groupe ne peut pas signaler son appartenance au groupe, ou il n'y a aucun membre d'un groupe sur le segment de réseau, mais vous souhaitez tout de même que le trafic de multidiffusion de ce groupe soit envoyé à ce segment de réseau. Vous pouvez envoyer le trafic de multidiffusion pour ce groupe au segment en configurant un groupe IGMP rejoint statiquement. Avec cette méthode, le périphérique défense contre les menaces 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 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **IGMP (IGMP)**.

Étape 3 Dans le **groupe statique**, cliquez sur **Add** ou **Edit**(ajouter ou modifier).

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

Remarque Le groupe statique IGMP 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.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface** (interface), choisissez l'interface à laquelle vous souhaitez affecter de manière statique un groupe de multidiffusion. Si vous modifiez une entrée existante, vous ne pouvez pas modifier la valeur.
- Dans la liste déroulante **Groupes de multidiffusion**, choisissez le groupe de multidiffusion auquel vous souhaitez affecter l'interface ou cliquez sur **Ajouter** (+) pour créer un nouveau groupe de multidiffusion. Reportez-vous à la section Création d'objets de réseau pour connaître la procédure.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du groupe statique.

Configurer des groupes de jonction IGMP

Vous pouvez configurer une interface pour qu'elle soit membre d'un groupe de multidiffusion. La configuration du périphérique défense contre les menaces pour se joindre à un groupe de multidiffusion fait en sorte que les routeurs en amont conservent les informations de la table de routage de multidiffusion pour ce groupe et maintiennent les chemins de ce groupe actifs.

Remarque Consultez Configurer des groupes statiques IGMP, à la page 10 si vous souhaitez transférer des paquets en multidiffusion pour un groupe spécifique vers une interface sans que le périphérique défense contre les menaces n'accepte ces paquets dans le cadre du groupe.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **IGMP (IGMP)**.

Étape 3 Dans la zone **Join Group** (Rejoindre le groupe), cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add IGMP Join Group parameters** (Ajouter les paramètres du groupe de jonction IGMP) pour configurer le périphérique défense contre les menaces pour qu'il soit membre d'un groupe de multidiffusion. Utilisez la boîte de dialogue **Edit IGMP Join Group Parameters** (Modifier les paramètres du groupe de jonction IGMP) pour modifier les paramètres existants.

Remarque Le groupe de jonction IGMP 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.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface** (interface), choisissez l'interface qui doit être membre d'un groupe de multidiffusion. Si vous modifiez une entrée existante, vous ne pouvez pas modifier la valeur.

- Dans la liste déroulante **Join Group** (Rejoindre le groupe) , choisissez le groupe de multidiffusion auquel vous souhaitez affecter l'interface, ou cliquez sur **Plus** pour créer un nouveau groupe de multidiffusion. Reportez-vous à la section Création d'objets de réseau pour connaître la procédure.

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 Appareil Cisco Secure Firewall Threat Defense, 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.

Procédure

Étape 1 Configurer le protocole PIM, à la page 12.
Étape 2 Configurer les filtres de voisinage PIM, à la page 13.
Étape 3 Configurer les filtres de voisinage bidirectionnels PIM, à la page 14.
Étape 4 Configurer les points de rendez-vous PIM, à la page 15.
Étape 5 Configurer les arborescences de routage PIM, à la page 16.
Étape 6 Configurer les filtres de demande PIM, à la page 17.
Étape 7 Configurer les filtres de limites de multidiffusion, à la page 20.

Configurer le protocole PIM

Vous pouvez activer ou désactiver PIM sur une interface spécifique.

Vous pouvez également configurer la priorité des routeurs désignés (DR). 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, le choix du routeur de priorité désignée 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, le périphérique défense contre les menaces a une priorité DR de 1.

Les messages de requête de routeur sont utilisés pour choisir 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, le périphérique défense contre les menaces envoie des messages de jonction ou suppression PIM.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Dans le menu **Protocol** (protocole), cliquez sur **Add** (ajouter) ou **Edit** (modifier).

Utilisez la boîte de dialogue **Add PIM settings** (ajouter des paramètres PIM) pour ajouter de nouveaux paramètres PIM à l'interface. Utilisez la boîte de dialogue **Edit PIM settings** pour modifier les paramètres PIM existants.

Étape 4 Configurez les options suivantes :

- **Interface** : Dans la liste déroulante, sélectionnez l'interface pour laquelle vous souhaitez configurer le protocole PIM.
- **Enable PIM**(activer PIM) : Cochez la case pour activer PIM.
- **DR Priority**(Priorité DR) : la valeur de la DR 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 du périphérique défense contre les menaces ne peut pas devenir le routeur désigné.
- **Hello Interval** : l'intervalle en secondes auquel l'interface envoie des messages PIM Hello. La plage est comprise entre 1 et 3600. La valeur par défaut est 30.
- **Join Prune Interval** (intervalle de suppression des jonctions) : intervalle en secondes auquel l'interface envoie des annonces de jonction et d'élimination PIM. La plage est comprise entre 10 et 600. La valeur par défaut est 60.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du protocole PIM.

Configurer les filtres de voisinage 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 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing** > **Multicast Routing** > **PIM** (Routage > Routage de multi-diffusion > PIM).

Étape 3 Dans **Neighbor Filter** (filtre de voisinage), cliquez sur **Add** ou **Edit** (ajouter ou modifier).

Utilisez la boîte de dialogue **Add PIM Neighbor Filter** (ajouter un filtre PIM de voisinage) pour ajouter de nouveaux filtres de voisinage PIM à l'interface. Utilisez la boîte de dialogue de modification du **filtre de voisinage PIM** pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface**, choisissez l'interface à laquelle vous souhaitez ajouter un filtre voisin PIM.
- **Standard Access List**(liste d'accès standard) : dans la liste déroulante **Standard Access List** (liste d'accès standard), choisissez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard pour connaître la procédure.

  Remarque Choisissez **Allow** (autoriser) dans la boîte de dialogue **Add Standard Access List entry** (ajouter une entrée de liste d'accès standard) pour permettre aux annonces de groupe de multidiffusion de passer par l'interface. Si vous choisissez **Block** (blocage), 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 Cliquez sur **OK** pour enregistrer la configuration de filtre de voisinage PIM.

Configurer les filtres de voisinage bidirectionnels PIM

Un filtre voisin bidirectionnel PIM est une liste de contrôle d'accès qui définit les périphériques voisins qui peuvent participer au choix du transitaire désigné (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.

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 dans les deux sens pour élire un DF.

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 de DF n'a pas lieu.
- Si un voisin refusé prend en charge le mode bidirectionnel, le choix DF ne se produit pas.
- Si un voisin refusé ne prend pas en charge le mode bidirectionnel, le choix DF peut se produire.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Multicast Routing** > **PIM** (Routage de multi-diffusion > PIM).

Étape 3 Dans le champ **Bidirectional Neighbor Filter** (filtre bidirectionnel de voisin), cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add PIM Bidirectional Neighbor Filter** (ajouter le filtre bidirectionnel de voisin PIM) pour créer des entrées ACL pour l'ACL du filtre bidirectionnel de voisin PIM. Utilisez la boîte de dialogue du **Edit PIM Bidirectional Neighbor Filter** (Modifier le filtre de voisin bidirectionnel PIM) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface** (interface), sélectionnez l'interface pour laquelle vous souhaitez configurer l'entrée d'ACL du filtre de voisin bidirectionnel PIM.
- **Standard Access List**(liste d'accès standard) : dans la liste déroulante **Standard Access List** (liste d'accès standard), sélectionnez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard pour connaître la procédure.

  Remarque Si vous choisissez **Allow** (autoriser) dans la boîte de dialogue **Add Standard Access List entry** (ajouter une entrée de liste d'accès standard) pour permettre aux périphériques spécifiés de participer au processus de sélection de la reprise après sinistre. Si vous choisissez **Block** (Bloquer), les périphériques spécifiés ne participent pas au processus de sélection de la reprise après sinistre.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du filtre du voisin bidirectionnel PIM.

Configurer les points de rendez-vous PIM

Vous pouvez configurer le périphérique défense contre les menaces pour qu'il serve de RP 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). Consultez Multidiffusion bidirectionnelle PIM, à la page 3 pour plus d'informations sur la PIM bidirectionnelle.

Les limitations et restrictions suivantes s'appliquent aux RP :

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

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Dans **Rendezvous Points** (Points de rendez-vous), cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add Rendezvous Point** (ajouter un point de rendez-vous) pour créer une nouvelle entrée dans le tableau Rendezvous Point. Utilisez la boîte de dialogue **Edit Rendezvous Point** (Modifier les points de rendez-vous) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Rendezvous Point IP address** (adresse de point de rendez-vous) , choisissez l'adresse IP que vous souhaitez ajouter en tant que RP ou cliquez sur **Ajouter** (+) pour créer un nouvel objet réseau. Reportez-vous à la section Création d'objets de réseau pour connaître la procédure.
- Cochez la case **Use bi-directionnel forwarding** (Utiliser le transfert bidirectionnel) si les groupes de multidiffusion spécifiés doivent fonctionner en mode bidirectionnel. En mode bidirectionnel, si le périphérique défense contre les menaces 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.
- Cliquez sur **Use this RP for all Multicast Groups** (utiliser ce RP pour tous les groupes de multidiffusion) afin d'utiliser le RP spécifié pour tous les groupes de multidiffusion sur l'interface.
- Cliquez sur le bouton **Use this RP for all Multicast Groups as specified below** (Utiliser ce RP pour tous les groupes de multidiffusion comme spécifié ci-dessous) pour désigner les groupes de multidiffusion à utiliser avec le RP spécifié, puis dans la liste déroulante **Standard Access List** (liste d'accès standard), choisissez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard pour connaître la procédure.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du point de rendez-vous.

Configurer les arborescences de routage PIM

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 le périphérique défense contre les menaces 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.

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.

Remarque Ce comportement est connu sous le nom de commutation SPT (Shortest Path Switchover) (Commutation du chemin le plus court). Nous vous recommandons de toujours utiliser l'option de l'arborescence partagée.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Sur **Route Tree** (Arborescence de routage), sélectionner le chemin pour l'arborescence de routage :

- Cliquez sur **Shortest Path** pour utiliser l'arborescence du chemin le plus court pour tous les groupes de multidiffusion.
- Cliquez sur **Shared Tree** (Arborescence partagée) pour utiliser l'arborescence partagée pour tous les groupes de multidiffusion.
- Cliquer sur **Shared tree for below mentioned group** l'arborescence partagée pour le groupe mentionné ci-dessous afin de désigner les groupes spécifiés dans le tableau Groupes de multidiffusion, puis dans la liste déroulante **Standard Access List** (liste d'accès standard), sélectionnez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard pour connaître la procédure.

Étape 4 Cliquez sur **OK** pour enregistrer la configuration d'arborescence de routage.

Configurer les filtres de demande PIM

Lorsque le périphérique défense contre les menaces agit comme un point de rendez-vous RP, vous pouvez empêcher certaines sources en multidiffusion de s'enregistrer auprès de lui pour empêcher les sources non autorisées de s'enregistrer auprès du RP. Vous pouvez définir les sources en multidiffusion dont le périphérique défense contre les menaces accepte les messages de registre PIM.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Dans **Request Filter** (filtre de requêtes), définissez les sources de multidiffusion qui sont autorisées à s'enregistrer auprès du périphérique défense contre les menaces lorsqu'il agit en tant que RP :

- Dans la liste déroulante **Filter PIM register messages using:** (Filtrer les messages de registre PIM en utilisant :), sélectionnez **None**, **Access List** ou **Route Map**.
- Si vous choisissez **Access List** (liste d'accès) dans la liste déroulante, sélectionnez une ACL étendue ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL étendue. Reportez-vous à Configurer les objets ACL étendus pour connaître la procédure.

  Remarque Dans la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), sélectionner **Allow** (autoriser) dans la liste déroulante pour créer une règle qui permet à la source précisée du trafic de multidiffusion précisé de s'enregistrer auprès du périphérique défense contre les menaces , ou sélectionnez **Block** (Bloquer)pour créer une règle qui empêche la source spécifiée du trafic de multidiffusion spécifié de s'enregistrer auprès de l'appareil.

- Si vous choisissez **Route Map** (carte de routage), sélectionnez une carte de routage dans la liste déroulante **Route Map** ou cliquez sur **Ajouter** (+) pour créer une nouvelle carte de routage. Reportez-vous à la section Création d'objets de réseau pour connaître la procédure.

Étape 4 Cliquez sur **OK** pour enregistrer la configuration du filtre de requête.

Configurer le périphérique Cisco Secure Firewall Threat Defense en tant que routeur candidat de démarrage

Vous pouvez configurer le périphérique défense contre les menaces en tant que BSR candidat.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM**.

Étape 3 Sur **Bootstrap Router** (Routeur de démarrage), cochez la case **Configure this FTD as a Candidate Bootstrap Router (C-BSR)** (Configurer ce FTD en tant que routeur de démarrage candidat) pour effectuer la configuration de C-BSR.

a) Dans la liste déroulante **Interface**, sélectionnez l'interface sur le périphérique défense contre les menaces dont l'adresse BSR est dérivée pour en faire une interface candidate.

Cette interface doit être activée avec PIM.

b) Dans le champ **Hash Mask long** (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 RP (Point de rendez-vous). 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. La valeur doit être comprise entre 0 et 32.

c) Dans le champ **Priority** (Priorité), saisissez la priorité du BSR candidat. 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 doit être comprise entre 0 et 255. La valeur par défaut est 0.

Étape 4 (Facultatif) Cliquez sur **Ajouter** (+) pour sélectionner une interface sur laquelle aucun message PIM BSR ne sera envoyé ou reçu dans la section **Configure this FTD as a Border Bootstrap Router (BSR)** (Configurer ce FTD en tant que Routeur de démarrage de frontière (BSR)).

- Dans la liste déroulante **Interface** (interface), sélectionnez l'interface sur laquelle aucun message PIM BSR ne sera envoyé ou reçu.

  Les annonces RP ou BSR sont filtrées, isolant ainsi deux domaines d'échange d'informations RP.

- Cochez la case **Enable Border BSR** (activer le BSR de frontière) pour activer BSR.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du routeur de démarrage.

Configurer le routage de multidiffusion

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, le périphérique défense contre les menaces 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 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routage** > **Routage de multidiffusion** > **routes de multidiffusion** > **Ajouter ou Modifier**.

Utilisez la boîte de dialogue **Ajouter la configuration d'une route de multidiffusion** pour ajouter une nouvelle route de multidiffusion au périphérique défense contre les menaces . Utilisez la boîte de dialogue **Edit Multicast Route Configuration** (modifier une configuration de route de multidiffusion) pour modifier une route de multidiffusion existante.

Étape 3 Dans la liste déroulante **Source Network** (réseau source), choisissez un réseau existant ou cliquez sur **Ajouter** (+) pour en ajouter un nouveau. Reportez-vous à la section Création d'objets de réseau pour connaître la procédure.

Étape 4 Pour configurer une interface afin de transférer le routage, cliquez sur **Interface** et configurez les options suivantes :

- Dans la liste déroulante **Source Interface** (interface source), choisissez l'interface entrante pour la route de multidiffusion.
- Dans la liste déroulante **Output Interface/Dense** (interface de sortie/Dense), choisissez l'interface de destination par laquelle la voie de routage est transférée.
- Dans le champ **Distance**, saisissez la distance de la route de multidiffusion. La valeur doit être comprise entre 0 et 255.

Étape 5 Pour configurer une adresse RPF afin de transférer la route, cliquez sur **Address** (adresse) et configurez les options suivantes :

- Dans le champ **RPF Address** (adresse RPF), saisissez l'adresse IP pour la route de multidiffusion.
- Dans le champ **Distance**, saisissez la distance de la route de multidiffusion. La plage s'étend de 0 à 255.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration des routes de multidiffusion.

Configurer les filtres de limites de multidiffusion

La portée des adresses définit des filtres de délimitation 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 un filtre 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'un filtre de limite est configuré, aucun paquet de données en multidiffusion ne peut traverser la limite dans aucune direction. Le filtre de 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 le filtre de 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 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **Multicast Boundary Filter (Filtre de limite de multidiffusion)**, puis cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add Multicast Boundary Filter** (ajouter un filtre de limite de multidiffusion) pour ajouter de nouveaux filtres de limite de multidiffusion au périphérique. Utilisez la boîte de dialogue de **modification du filtre de limite de multidiffusion** pour modifier les paramètres existants.

Vous pouvez 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 3 Dans la liste déroulante **Interface** (interface), choisissez l'interface pour laquelle vous configurez la liste de contrôle d'accès du filtre de limite de multidiffusion.

Étape 4 Dans la liste déroulante **Standard Access List** (liste d'accès standard), choisissez la liste de contrôle d'accès standard que vous souhaitez utiliser ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard pour connaître la procédure.

Étape 5 Cochez la case **Supprimez toute annonce de plage de groupes Auto-RP des paquets Auto-RP refusés par la limite** pour filtrer les messages Auto-RP des sources refusées par la liste de contrôle d'accès (ACL) de la limite. Si cette case n'est pas cochée, tous les messages Auto-RP sont transmis.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration du filtre de limite de multidiffusion.

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.