RIP

Ce chapitre décrit comment configurer défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole RIP (Routing Information Protocol). Pour un périphérique utilisant le routage virtuel, vous pouvez configurer RIP uniquement pour son routeur virtuel global et non pour son routeur virtuel défini par l'utilisateur.

À propos de RIP

Le protocole de routage des informations de routage (RIP), comme on l'appelle plus communément, est l'un des plus endurants de tous les protocoles de routage. IP comporte quatre composants de base : le processus de mise à jour du routage, les mesures de routage, la stabilité du routage et les minuteries de routage. Le protocole RIP envoie des messages de mise à jour du routage à intervalles réguliers et lorsque la topologie du réseau change. Ces paquets RIP comprennent des informations sur les réseaux que les périphériques peuvent atteindre, ainsi que sur le nombre de routeurs ou de passerelles qu'un paquet doit traverser pour atteindre l'adresse de destination. RIP génère plus de trafic qu'OSPF, mais est plus facile à configurer.

RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme mesure pour la sélection de chemin. Lorsque RIP est activé sur une interface, l'interface échange des diffusions IPS avec les périphériques voisins pour obtenir des renseignements sur les routages et les annoncer de manière dynamique.

L'Appareil Cisco Secure Firewall Threat Defense prend en charge à la fois la version 1 et la version 2 de RIP. RIP version 1 n'envoie pas le masque de sous-réseau avec la mise à jour du routage. La version 2 de RIP envoie le masque de sous-réseau avec la mise à jour du routage et prend en charge les masques de sous-réseau de longueur variable. De plus, la version 2 de RIP prend en charge l'authentification du voisin lors de l'échange des mises à jour de routage. Cette authentification garantit que l'Appareil Cisco Secure Firewall Threat Defense reçoit des informations de routage fiables provenant d'une source de confiance.

RIP présente des avantages par rapport aux routes statiques, car la configuration initiale est simple et vous n'avez pas besoin de mettre à jour la configuration lorsque la topologie change. L'inconvénient de RIP est qu'il a plus de surdébit de réseau et de traitement que le routage statique.

Processus de mise à jour du routage

Le protocole RIP envoie des messages de mise à jour du routage à intervalles réguliers et lorsque la topologie du réseau change. Lorsqu'un routeur reçoit une mise à jour de routage qui inclut des modifications apportées à une entrée, il met à jour sa table de routage pour refléter la nouvelle route. La valeur de la métrique pour le chemin est incrémentée de 1 et l'expéditeur est indiqué comme le prochain saut. Les routeurs RIP ne maintiennent que la meilleure route (la route avec la valeur de métrique la plus basse) vers une destination. Après avoir mis à jour sa table de routage, le routeur commence immédiatement à transmettre les mises à jour de routage pour informer les autres routeurs du réseau du changement. Ces mises à jour sont envoyées indépendamment des mises à jour régulières envoyées par les routeurs RIP.

Mesure de routage RIP

RIP utilise une seule métrique de routage (nombre de sauts) pour mesurer la distance entre le réseau source et le réseau de destination. Chaque saut d'un chemin, de la source à la destination, se voit attribuer une valeur de nombre de sauts, qui est généralement de 1. Lorsqu'un routeur reçoit une mise à jour de routage qui contient une nouvelle entrée de réseau de destination ou une entrée modifiée, le routeur ajoute 1 à la valeur de la métrique indiquée dans la mise à jour et inscrit le réseau dans la table de routage. L'adresse IP de l'expéditeur est utilisée comme saut suivant.

Fonctionnalités de stabilité RIP

Le IPS empêche les boucles de routage de se poursuivre indéfiniment en mettant en œuvre une limite sur le nombre de sauts autorisés dans un chemin, de la source à la destination. Le nombre maximal de sauts dans un chemin est de 15. Si un routeur reçoit une mise à jour de routage qui contient une nouvelle entrée ou une entrée modifiée, et si l'augmentation de la valeur de la métrique de 1 fait que la métrique a la valeur infinie (c'est-à-dire 16), la destination réseau est considérée comme inaccessible. L'inconvénient de cette fonctionnalité de stabilité est qu'elle limite le diamètre maximal d'un réseau IPS à moins de 16 sauts.

IPS comprend un certain nombre d'autres fonctionnalités de stabilité communes à de nombreux protocoles de routage. Ces fonctionnalités sont conçues pour assurer la stabilité malgré les changements potentiellement rapides dans la topologie du réseau. Par exemple, le IPS met en œuvre les mécanismes de partage d' horizon et de maintien pour empêcher la propagation d' informations de routage incorrectes.

Temporisateurs RIP

Le RIP utilise des temporisateurs pour régler sa performance. Voici les étapes de minuterie de RIP :

- Update (mise à jour) : la minuterie de mise à jour de routage correspond à l'intervalle entre les mises à jour périodiques du routage. Il s'agit de la fréquence à laquelle le périphérique envoie des mises à jour de routage. En général, elle est réglée à 30 secondes, avec une petite durée aléatoire ajoutée chaque fois que la minuterie est réinitialisée. Ceci est fait pour aider à éviter la congestion, qui pourrait résulter du fait que tous les routeurs tentent simultanément de mettre à jour leurs voisins.
- Invalid (Non valide) : chaque entrée de la table de routage est associée à un minuteur de délai d'expiration de routage. Il s'agit du nombre de secondes depuis que le périphérique a reçu la dernière mise à jour valide. Lorsque le délai d'expiration du routage expire, le routage est marqué comme non valide mais est conservé dans le tableau jusqu'à l'expiration de la minuterie de vidage de routage. Une fois cette minuterie expirée, la voie de routage passe en attente. La valeur par défaut est 600 secondes (10 minutes).

- Holddown (Maintien) : la période de maintien est le nombre de secondes pendant lesquelles le système attend avant d'accepter de nouvelles mises à jour pour le routage en attente (c'est-à-dire les routages marqués non valides). La valeur par défaut est 600 secondes (10 minutes).
- Flush (Purge) : la minuterie de vidage de routage est le nombre de secondes depuis que le système a reçu la dernière mise à jour valide jusqu'à ce que la voie de routage soit rejetée et supprimée de la table de routage. La valeur par défaut est 240 secondes (4 minutes).

Par exemple, lorsque l'interface d'un routeur adjacent tombe en panne, le système ne reçoit plus les mises à jour de routage du routeur adjacent. À ce stade, les minuteries non valide et de purge commencent à augmenter. Pendant les 180 premières secondes, rien ne se passera. Après 180 secondes, la minuterie de non-validité expire, ce qui rend la voie de routage non valide, et la minuterie de maintien démarre et retient la voie de routage pendant 60 autres secondes. S'il n'y a toujours pas de mise à jour concernant l'état de l'interface sur le routeur adjacent (c'est-à-dire s'il est toujours en panne), la voie de routage entre dans l'état de purge où au total, le système a attendu 240 secondes à partir de la dernière mise à jour (180 secondes pour la minuterie non valide et 60 secondes pour la minuterie de maintien) et le système purge la voie de routage. Même si l'interface du routeur adjacente s'active immédiatement, le système n'accepte pas de mise à jour du routage tant que la minuterie de maintien n'a pas terminé les 120 secondes restantes.

Exigences et prérequis RIP

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 RIP

Directives IPv6

Ne prend pas en charge IPv6.

Directives supplémentaires

Les informations suivantes s'appliquent uniquement à la version 2 de RIP :

- Si vous utilisez l'authentification par voisin, la clé d'authentification et l'ID de clé doivent être les mêmes sur tous les périphériques voisins qui fournissent les mises à jour de RIP version 2 à l'interface.

- Avec la version 2 de RIP, l'Appareil Cisco Secure Firewall Threat Defense transmet et reçoit les mises à jour de route par défaut en utilisant l'adresse de multidiffusion 224.0.0.9. En mode passif, il reçoit les mises à jour de routage à cette adresse.
- Lorsque RIP version 2 est configuré sur une interface, l'adresse de multidiffusion 224.0.0.9 est enregistrée sur cette interface. Lorsqu'une configuration RIP version 2 est supprimée d'une interface, cette adresse de multidiffusion est non enregistrée.

Restrictions

- L'Appareil Cisco Secure Firewall Threat Defense ne peut pas transmettre les mises à jour RIP entre les interfaces.
- La version 1 de RIP ne prend pas en charge les masques de sous-réseau de longueur variable.
- Le nombre de sauts maximal est de 15. Une route avec un nombre de sauts supérieur à 15 est considérée comme inaccessible.
- La convergence RIP est relativement lente par rapport à d'autres protocoles de routage.
- Vous ne pouvez activer qu'un seul processus IPS sur Appareil Cisco Secure Firewall Threat Defense.

Configurer RIP

RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme mesure pour la sélection de chemin.

Procédure

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

Étape 2 Sélectionnez **Routing**(Routage).

Étape 3 Sélectionnez **RIP** dans la table des matières.

Étape 4 Cochez la case **Enable RIP** (activer RIP) pour configurer les paramètres RIP.

Étape 5 Choisissez les versions de IPS pour l'envoi et la réception des mises à jour dans la liste déroulante **RIP Version**.

Étape 6 (Facultatif) Cochez la case **Generate Default Route** (générer une route par défaut) pour générer une route par défaut pour la distribution, en fonction de la carte de routage que vous spécifiez.

a) Spécifiez un nom de carte de routage à utiliser pour générer des routes par défaut dans le champ **Route Map**.
La route par défaut 0.0.0.0/0 est générée pour la distribution sur une certaine interface lorsque la carte de routage, spécifiée dans le champ **Route Map**, est présente.

Étape 7 Lorsque la version d'envoi et de réception de la version 2 est la version IP choisie, l'option **Enable Auto Summary** (activer le résumé automatique) est disponible. Lorsque la **case Enable Auto Summary** (activer le résumé automatique) est cochée, le résumé automatique du routage est activé. Désactivez la récapitulation automatique si vous devez effectuer le routage entre des sous-réseaux déconnectés. Lorsque la récapitulation automatique est désactivée, les sous-réseaux sont annoncés.

Remarque RIP version 1 utilise toujours la récapitulation automatique : vous ne pouvez pas la désactiver.

Étape 8 Cliquez sur **Networks** (Réseaux). Définissez un ou plusieurs réseaux pour le routage RIP. Saisissez les adresses IP ou saisissez ou sélectionnez les objets réseau ou les hôtes souhaités. Il n'y a aucune limite au nombre de réseaux que vous pouvez ajouter à la configuration du périphérique de sécurité. Toute interface appartenant à un réseau défini par cette commande participera au processus de routage IPS. Les mises à jour du routage IPS seront envoyées et reçues uniquement par l'intermédiaire d'interfaces sur les réseaux spécifiés. De plus, si le réseau d'une interface n'est pas précisé, l'interface ne sera annoncée dans aucune mise à jour RIP.

Remarque RIP ne prend en charge que les objets IPv4.

Étape 9 (Facultatif) Cliquez sur **Passive Interface** (interface passive). Utilisez cette option pour préciser les interfaces passives du périphérique et, par extension, les interfaces actives. Le périphérique écoute les diffusions de routage IP sur les interfaces passives, et utilise ces informations pour remplir ses tableaux de routage, mais ne diffuse pas de mises à jour de routage sur les interfaces passives. Les interfaces qui ne sont pas désignées comme passives reçoivent et envoient des mises à jour.

Étape 10 Cliquez sur **Redistribution** pour gérer les routages de redistribution. Il s'agit des routes redistribuées à partir d'autres processus de routage vers le processus de routage RIP.

a) Cliquez sur **Add** pour spécifier les routes de redistribution.

b) Choisissez le protocole de routage à redistribuer dans le processus de routage RIP dans la liste déroulante **Protocol** (protocole).

Remarque Pour le protocole OSPF, spécifiez un ID de processus. De même, spécifiez un chemin de système autonome pour BGP. Lorsque vous choisissez l'option Connected (Connecté) dans la liste déroulante **Protocol** (protocole), vous pouvez redistribuer les réseaux directement connectés dans le processus de routage RIP.

c) (Facultatif) Si vous redistribuez les routes OSPF dans le processus de routage IP, vous pouvez sélectionner des types spécifiques de routes OSPF à redistribuer dans la liste déroulante **Correspondance**. Tout en maintenant la touche Ctrl enfoncée pour sélectionner plusieurs types :

- **Internal** (Interne) : les routes internes au système autonome (AS) sont redistribuées.
- **Externe 1** : les routages de type 1 externes au système autonome sont redistribués.
- **Externe 2** : les routes de type 2 externes au système autonome sont redistribuées.
- **NSSA externe 1** : les routages de type 1 externes vers une zone non-so-stubby (NSSA) sont redistribués.
- **NSSA externe 2** : les routages de type 2 externes vers une zone NSSA sont redistribués

Remarque La valeur par défaut est Interne, Externe 1 et Externe 2

d) Sélectionnez le type de mesure RIP à appliquer aux routages redistribués dans la liste déroulante **Metric** (Métrique). Les deux choix sont :

- **Transparent** : utilisez la métrique de route actuelle
- **Valeur précisée** : attribue une valeur métrique précise. Saisissez une valeur comprise entre 0 et 16 dans le champ **Metric Value** (valeur de la métrique).
- **Aucune** : aucune mesure n'est spécifiée. N'utilisez aucune valeur de mesure à appliquer aux routages redistribués.

Remarque L'option Aucune s'applique uniquement aux protocoles Static et Connected.

e) (Facultatif) Dans le champ **Route Map**, saisissez le nom d'une carte de routage qui doit être respectée avant que la route puisse être redistribuée dans le processus de routage RIP. Les routes sont redistribuées uniquement si l'adresse IP correspond à une instruction Allow (autorisation) dans la liste d'adresses de la carte de routage. Pour créer un nouvel objet de carte de routage, cliquez sur **Ajouter** (+). Voir Configurer l'entrée de la carte de routage pour connaître la procédure d'ajout d'une nouvelle carte de routage.

f) Cliquez sur **OK**.

Étape 11 (Facultatif) Cliquez sur **Filtering** (filtrage) pour gérer les filtres de la politique RIP. Dans cette section, les filtres sont utilisés pour empêcher les mises à jour de routage de traverser une interface, contrôler la publicité des routages dans les mises à jour de routage, contrôler le traitement des mises à jour de routage et filtrer les sources des mises à jour de routage.

a) Cliquez sur **Add** (ajouter) pour ajouter des filtres RIP.

b) Sélectionnez le type de trafic à filtrer (entrée ou sortie) dans le champ **Traffic Direction** .

Remarque Si le trafic est entrant, vous pouvez uniquement définir un filtre d'interface.

c) Précisez si le filtre est basé sur une interface ou une voie de routage, en sélectionnant l'option appropriée dans le champ **Filtrer sur**. Si vous cliquez sur **Interface**, saisissez ou choisissez le nom de l'interface sur laquelle les mises à jour de routage doivent être filtrées. Si vous cliquez sur **Routage**, choisissez le type de routage :

- **Statique** : seules les routes statiques sont filtrées.
- **Connecté** : seules les routes connectées sont filtrées.
- **OSPF** : seules les routes OSPFv2 découvertes par le processus OSPF spécifié sont filtrées. Saisissez l'ID de processus du processus OSPF à filtrer.
- **BGP** : seules les routes BGPv4 découvertes par le processus BGP spécifié sont filtrées. Saisissez le chemin de système autonome du processus BGP à filtrer.

d) Dans le champ **Access List** (liste d'accès), saisissez ou choisissez le nom d'une ou de plusieurs listes de contrôle d'accès (ACL) qui définissent les réseaux à autoriser ou à supprimer des annonces de routage RIP. Pour ajouter un nouvel objet de liste d'accès standard, cliquez sur **Ajouter** (+) et consultez Configurer les objets ACL standard.

e) Cliquez sur **OK**.

Étape 12 (Facultatif) Cliquez sur **Broadcast** (diffuser) pour ajouter ou modifier des configurations d'interface. À l'aide de la diffusion, vous pouvez remplacer les versions RIP globales pour envoyer ou recevoir par interface. Vous pouvez également définir les paramètres d'authentification par interface si vous souhaitez mettre en œuvre l'authentification pour garantir des mises à jour RIP valides.

a) Cliquez sur **Ajouter** pour enregistrer les configurations.

b) Saisissez ou choisissez une interface définie sur cet appareil dans le champ **Interface**.

c) Dans l'option Send (envoyer), cochez les cases appropriées pour spécifier l'envoi des mises à jour à l'aide de la **version 1**, de la **version 2**ou des deux . Ces options vous permettent de remplacer, pour l'interface spécifiée, les versions d'envoi globales spécifiées .

d) Dans l'option Receive (réception), cochez les cases appropriées pour préciser l'acceptation des mises à jour à l'aide de RIP **version 1**, **version 2**ou les deux. Ces options vous permettent de remplacer, pour l'interface spécifiée, les versions globales de réception spécifiées.

e) Sélectionnez l'**authentification** utilisée sur cette interface pour les diffusions RIP.

- **None** : aucune authentification
- **MD5** : utilisez MD5
- **Clear Text** : utilisez l'authentification en texte clair

Si vous choisissez MD5 ou Clear Text, vous devez également fournir les paramètres d'authentification suivants.

- **Key ID** (ID de clé) : ID de la clé d'authentification. Les valeurs valides sont comprises entre 0 et 255.
- **Clé** : la clé utilisée par la méthode d'authentification choisie. Peut contenir jusqu'à 16 caractères
- **Confirmer** – Saisissez à nouveau la clé d'authentification pour confirmer

f) Cliquez sur **OK**.

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.