Routages statiques et par défaut

Ce chapitre décrit comment configurer les routes statiques et par défaut sur défense contre les menaces .

À propos des routages statiques et par défaut

Pour acheminer le trafic vers un hôte ou un réseau non connecté, vous devez définir une voie de routage vers l'hôte ou le réseau, à l'aide du routage statique ou dynamique. En général, vous devez configurer au moins une route statique : une route par défaut pour tout le trafic qui n'est pas acheminé par d'autres moyens vers une passerelle de réseau par défaut, en général le routeur du saut suivant.

Routage par défaut

L'option la plus simple est de configurer une voie de routage statique par défaut pour envoyer tout le trafic vers un routeur en amont, en se fondant sur le routeur pour acheminer le trafic à votre place. Une voie de routage par défaut identifie l'adresse IP de la passerelle à laquelle appareil de défense contre les menaces envoie tous les paquets IP pour lesquels il n'a pas de voie de routage statique ou apprise. Une voie de routage statique par défaut est simplement une voie de routage statique avec 0.0.0.0/0 (IPv4) ou::/0 (IPv6) comme adresse IP de destination.

Vous devez toujours définir une voie de routage par défaut.

Comme défense contre les menaces utilise des tables de routage distinctes pour le trafic de données et pour le trafic de gestion, vous pouvez éventuellement configurer une voie de routage par défaut pour le trafic de données et une autre voie de routage par défaut pour le trafic de gestion. Notez que le trafic provenant du périphérique utilise par défaut la table de routage de gestion uniquement ou de données, en fonction du type (voir Table de routage pour le trafic de gestion, à la page 14), mais qu'il revient à l'autre table de routage si aucune route n'est trouvée. Les routes par défaut correspondront toujours au trafic et empêcheront un recours à l'autre table de routage. Dans ce cas, vous devez préciser l'interface que vous souhaitez utiliser pour le trafic de sortie si cette interface ne figure pas dans la table de routage par défaut. L'interface de dépistage est incluse dans le tableau des valeurs de gestion uniquement. L'interface de gestion spéciale utilise une table de routage Linux distincte et possède sa propre voie de routage par défaut. Consultez les commandes **configure network**.

Routes statiques

Vous pourriez souhaiter utiliser des routes statiques dans les cas suivants :

- Vos réseaux utilisent un protocole de découverte de routeur non pris en charge.
- Votre réseau est de petite taille et vous pouvez facilement gérer des routes statiques.
- Vous ne voulez pas associer le trafic ou la surcharge de la CPU aux protocoles de routage.
- Dans certains cas, une route par défaut ne suffit pas. La passerelle par défaut peut ne pas être en mesure d'atteindre le réseau de destination, vous devez donc également configurer des routes statiques plus spécifiques. Par exemple, si la passerelle par défaut est externe, la voie de routage par défaut ne peut pas diriger le trafic vers des réseaux internes qui ne sont pas directement connectés à appareil de défense contre les menaces .
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.
- Les routeurs virtuels utilisent des routes statiques pour créer des fuites de route. Les fuites de route permettent le flux du trafic d'une interface d'un routeur virtuel vers une autre interface dans un autre routeur virtuel. Pour en savoir plus, consultez Interconnexion des routeurs virtuels.

Routage vers l'interface null0 pour abandonner le trafic indésirable

Les règles d'accès vous permettent de filtrer les paquets en fonction des informations contenues dans leurs en-têtes. Une voie de routage statique vers l'interface null0 est une solution complémentaire aux règles d'accès. Vous pouvez utiliser une route null0 pour transférer le trafic indésirable ou indésirable afin que le trafic soit abandonné.

Les routes statiques Null0 ont un profil de rendement positif. Vous pouvez également utiliser des routes statiques null0 pour éviter les boucles de routage. BGP peut tirer parti de la route statique null0 pour le routage trou noir déclenché à distance.

Priorités de routage

- Les routes qui identifient une destination spécifique prévalent sur la route par défaut.
- Lorsque plusieurs routages existent vers la même destination (statique ou dynamique), la distance administrative du routage détermine la priorité. Les routes statiques sont définies à 1, ce sont donc généralement les routes les plus prioritaires.
- Lorsque vous avez plusieurs routes statiques vers la même destination avec la même distance administrative, consultez Routage à chemins multiples à coûts égaux (ECMP)., à la page 15.
- Pour le trafic sortant d'un tunnel avec l'option tunnelisé, cette voie de routage remplace toute autre voie de routage par défaut configurée ou apprise.

Routages en mode de pare-feu transparent et de groupes de ponts

Pour le trafic qui provient du appareil de défense contre les menaces et est destiné à travers une interface membre de groupe de ponts pour un réseau non connecté directement, vous devez configurer une voie de routage par défaut ou des routes statiques pour que l'appareil de défense contre les menaces sache de quelle

interface membre de groupe de ponts envoyer trafic. Le trafic provenant de appareil de défense contre les menaces peut inclure des communications avec un serveur syslog ou SNMP. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques. Pour le mode transparent, vous ne pouvez pas spécifier les BVI comme interface de passerelle; seules les interfaces membres peuvent être utilisées. Pour les groupes de ponts en mode routé, vous devez préciser le BVI dans une voie de routage statique; vous ne pouvez pas définir d'interface membre. Consultez la #unique_1183 pour de plus amples renseignements.

Suivi du routage statique

L'un des problèmes des routes statiques est qu'il n'y a pas de mécanisme inhérent pour déterminer si la route est active ou inactive. Les routes statiques restent dans la table de routage même si la passerelle du saut suivant n'est plus disponible. Les routes statiques ne sont supprimées de la table de routage que si l'interface associée appareil de défense contre les menaces tombe en panne.

La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Par exemple, vous pouvez définir une route par défaut vers une passerelle de FAI et une route de secours par défaut vers un FAI secondaire au cas où le FAI principal deviendrait indisponible.

L'appareil de défense contre les menaces met en œuvre le suivi de route statique en associant une route statique à un hôte cible de surveillance sur le réseau de destination que l'appareil de défense contre les menaces surveille à l'aide des demandes Echo ICMP. Si aucune réponse écho n'est reçue dans un délai donné, l'hôte est considéré comme hors service et la route associée est supprimée de la table de routage. Une route de secours non suivie avec une métrique plus élevée est utilisée à la place de la route supprimée.

Lorsque vous sélectionnez une cible de surveillance, vous devez vous assurer qu'elle peut répondre aux demandes d'écho ICMP. La cible peut être n'importe quel objet réseau de votre choix, mais vous pouvez envisager d'utiliser les objets suivants :

- L'adresse de la passerelle du FAI, pour la prise en charge du double FAI.
- L'adresse de passerelle du saut suivant, si vous êtes préoccupé par la disponibilité de la passerelle.
- Un serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel l'appareil de défense contre les menaces doit communiquer.
- Un objet réseau persistant sur le réseau de destination

Remarque Un poste de travail qui peut être éteint la nuit n'est pas un bon choix.

Vous pouvez configurer le suivi de routage statique pour les routes définies de manière statique ou pour les routages par défaut obtenus par DHCP ou PPPoE. Vous pouvez uniquement activer les clients PPPoE sur plusieurs interfaces avec le suivi de routage configuré.

Exigences et conditions préalables pour les routages statiques

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices pour les routages statiques et par défaut

Mode de pare-feu et groupes de ponts

- En mode transparent, les routes statiques doivent utiliser l’interface du membre du groupe de ponts comme passerelle; vous ne pouvez pas préciser les BVI.
- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l’interface membre.
- Le suivi de routage statique n’est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

Adresse réseau prise en charge

- Le suivi de routage statique n’est pas pris en charge pour IPv6.
- L’ASA ne prend pas en charge le routage de CLASSE E. Par conséquent, les réseaux de CLASSE E ne peuvent pas être routés en tant que routes statiques.

Mise en grappe et mode de contexte multiple

- Dans la mise en grappe, le suivi de routage statique n’est pris en charge que sur l’unité principale.
- Le suivi de routage statique n’est pas pris en charge en mode de contexte multiple.

Groupe d’objets réseau

Vous ne pouvez pas utiliser une plage d’objets réseau ou un groupe d’objets réseau ayant une plage d’adresses IP lors de la configuration d’une voie de routage statique.

Entrées de routage ASP et RIB

Tous les routages et leur distance installés sur le périphérique sont capturés dans la table de routage ASP. Cette situation est commune à tous les protocoles de routage statiques et dynamiques. Seule la meilleure distance de routage est saisie dans le tableau RIB.

Ajouter une route statique

Une voie de routage statique définit où envoyer le trafic pour des réseaux de destination spécifiques. Vous devez au minimum définir une voie de routage par défaut. Une voie de routage par défaut est simplement une voie de routage statique avec 0.0.0.0/0 comme adresse IP de destination.

Procédure

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

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour les périphériques compatibles avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, sélectionnez le routeur virtuel pour lequel vous configurez une voie de routage statique.

Étape 4 Sélectionnez **Route statique**.

Étape 5 Cliquez sur **Add Routes** (ajouter des routages).

Étape 6 Cliquez sur **IPv4** ou **IPv6** en fonction du type de route statique que vous ajoutez.

Étape 7 Choisissez l'**interface** à laquelle cette voie de routage statique s'applique.

Pour le mode transparent, choisissez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, vous pouvez choisir l'interface de membre du groupe de ponts pour le nom des BVI. Pour « rendre invisible » le trafic indésirable, choisissez l'interface **Null0**.

Si vous avez activé le routage et le transfert virtuels, vous pouvez sélectionner une interface qui appartient à un autre routeur virtuel. Vous pouvez créer une telle voie de routage statique si vous souhaitez laisser fuiter le trafic de ce routeur virtuel vers l'autre routeur virtuel. Pour en savoir plus, consultez Interconnexion des routeurs virtuels.

Étape 8 Dans la liste des **réseaux disponibles**, choisissez le réseau de destination.

Pour définir une voie de routage par défaut, créez un objet avec l'adresse 0.0.0.0/0 et sélectionnez-la ici.

Remarque Bien que vous puissiez créer et choisir un groupe d'objets réseau contenant une plage d'adresses IP, centre de gestion ne prend pas en charge l'utilisation de la plage d'objets réseau lors de la configuration d'une voie de routage statique.

Étape 9 **Gateway (passerelle)** ou **IPv6 Gateway (passerelle iPv6)** : Saisissez ou choisissez le routeur de passerelle qui est le prochain saut sur cette voie de routage. Vous pouvez fournir une adresse IP ou un objet réseaux/hôtes. Lorsque vous utilisez une configuration de routage statique pour que les routeurs virtuels présentent une fuite de route, ne spécifiez pas la passerelle du saut suivant.

Étape 10 Dans le champ **Mesure**, entrez le nombre de sauts vers le réseau de destination. Les valeurs valides vont de 1 à 255; la valeur par défaut est 1. La mesure est une mesure des « dépenses » d'un routage, en fonction du nombre de sauts (nombre de sauts) vers le réseau sur lequel réside un hôte spécifique. Le nombre de sauts est le nombre de réseaux qu'un paquet réseau doit traverser, y compris le réseau de destination, avant d'atteindre sa destination finale. La métrique est utilisée pour comparer les routages entre les différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une voie de routage statique a la même distance administrative qu'une voie de routage dynamique, la voie statique prévaut. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Remarque Pour une configuration d'interface double ISP/WAN, vous devez affecter la même valeur de mesure pour les interfaces de données principale et secondaire. Par défaut, vous n'êtes pas autorisé à configurer la même valeur de métrique pour deux interfaces. Pour remplacer l'erreur de validation, vérifiez que les deux interfaces appartiennent à une seule zone ECMP.

Étape 11 (Facultatif) Pour une voie de routage par défaut, cochez la case **Tunneled** (en tunnel) pour définir une voie de routage par défaut distincte pour le trafic VPN.

Vous pouvez définir une voie de routage par défaut distincte pour le trafic VPN si vous souhaitez que votre trafic VPN utilise une voie de routage par défaut différente de celle du trafic non VPN. Par exemple, le trafic entrant des connexions VPN peut être facilement dirigé vers les réseaux internes, tandis que le trafic des réseaux internes peut être dirigé vers l'extérieur. Lorsque vous créez une voie de routage par défaut avec l'option tunnelisé, tout le trafic provenant d'un tunnel se terminant sur le périphérique qui ne peut pas être acheminé à l'aide de routes apprises ou statiques est envoyé vers cette voie de routage. Vous ne pouvez configurer qu'une seule passerelle de tunnellisation par défaut par périphérique. ECMP pour le trafic en tunnel n'est pas pris en charge.

Étape 12 (Route statique IPv4 uniquement) Pour surveiller la disponibilité de la voie de routage, saisissez ou choisissez le nom d'un objet Moniteur SLA (Service Level Agreement, contrat de niveau de service) qui définit la politique de surveillance dans le champ **Route Tracking** (Surveillance du routage).

Consultez Surveillance SLA.

Remarque Veillez à attribuer un SLA pour les routes statiques des interfaces de données principale et secondaire (configuration d'interface double ISP/WAN).

Étape 13 Cliquez sur **Ok**.

Référence pour le routage

Cette section décrit les concepts sous-jacents du comportement du routage dans défense contre les menaces .

Détermination du chemin

Les protocoles de routage utilisent des métriques pour évaluer quel chemin sera le meilleur à parcourir pour un paquet. Une métrique est une norme de mesure, telle que la bande passante du chemin, utilisée par les algorithmes de routage pour déterminer le chemin optimale vers une destination. Pour faciliter le processus de détermination du chemin, les algorithmes de routage lancent et gèrent les tableaux de routage, qui comprennent les informations de routage. Les informations de route varient en fonction de l'algorithme de routage utilisé.

Les algorithmes de routage remplissent les tableaux de routage avec diverses informations. Les associations de destination ou du prochain saut indiquent à un routeur qu'une destination particulière peut être atteinte de manière optimale en envoyant le paquet à un routeur particulier représentant le prochain saut sur le chemin vers la destination finale. Lorsqu'un routeur reçoit un paquet entrant, il vérifie l'adresse de destination et tente d'associer cette adresse à un saut suivant.

Les tableaux de routage peuvent également comprendre d'autres informations, telles que des données sur l'opportunité d'un chemin. Les routeurs comparent les métriques pour déterminer les routes optimales. Ces métriques varient en fonction de la conception de l'algorithme de routage utilisé.

Les routeurs communiquent entre eux et gèrent leurs tables de routage par la transmission de divers messages. Le message de mise à jour du routage en est un qui consiste généralement en tout ou en partie d'une table de routage. En analysant les mises à jour de routage de tous les autres routeurs, votre routeur peut dresser un tableau détaillé de la topologie du réseau. Une annonce d'état de lien, un autre exemple de message envoyé entre des routeurs, informe les autres routeurs de l'état des liens de l'expéditeur. Les informations sur la liaison peuvent également être utilisées pour dresser une image complète de la topologie du réseau afin de permettre aux routeurs de déterminer les routes optimales vers les destinations du réseau.

Types de routage pris en charge

Un routeur peut utiliser plusieurs types de routage. L'appareil de défense contre les menaces utilise les types de routage suivants :

- Statique ou dynamique
- Chemin unique ou chemin multiple
- Non hiérarchique ou hiérarchique
- État de lien ou vecteur de distance

Statique ou dynamique

Les algorithmes de routage statique sont en fait des mappages de tables établis par l'administrateur réseau. Ces mappages ne changent pas, sauf si l'administrateur réseau les modifie. Les algorithmes qui utilisent des routes statiques sont simples à concevoir et fonctionnent bien dans des environnements où le trafic réseau est relativement fiable et où la conception de réseau est relativement simple.

Étant donné que les systèmes de routage statique ne peuvent pas réagir aux modifications du réseau, ils sont généralement considérés comme ne convenant pas aux grands réseaux en constante évolution. La plupart des algorithmes de routage prédominants sont des algorithmes de routage dynamique, qui s'adaptent aux circonstances changeantes du réseau en analysant les messages de mise à jour de routage entrants. Si le message indique qu'un changement de réseau est survenu, le logiciel de routage recalcule les routages et envoie de nouveaux messages de mise à jour de routage. Ces messages pénètrent dans le réseau, incitant les routeurs à réexécuter leurs algorithmes et à modifier leurs tables de routage en conséquence.

Les algorithmes de routage dynamique peuvent être complétés par des routes statiques, le cas échéant. Un routeur de dernier recours (une voie de routage par défaut pour un routeur auquel tous les paquets non routables sont envoyés), par exemple, peut être désigné pour servir de référentiel pour tous les paquets non routables, garantissant que tous les messages sont au moins gérés d'une manière ou d'une autre.

Chemin unique ou chemin multiple

Certains protocoles de routage sophistiqués prennent en charge plusieurs chemins vers la même destination. Contrairement aux algorithmes à chemin unique, ces algorithmes à chemins multiples permettent le multiplexage du trafic sur plusieurs lignes. Les avantages des algorithmes par chemins multiples sont un débit et une fiabilité considérablement meilleurs, ce qui est généralement appelé partage de charge.

Non hiérarchique ou hiérarchique

Certains algorithmes de routage fonctionnent dans un espace à plat, tandis que d'autres utilisent des hiérarchies de routage. Dans un système de routage à plat, les routeurs sont les homologues de tous les autres. Dans un système de routage hiérarchique, certains routeurs forment ce qui équivaut à un réseau fédérateur (backbone) de routage. Les paquets provenant de routeurs ne faisant pas partie du réseau fédérateur sont acheminés vers les routeurs de ce dernier, où ils sont envoyés à travers le réseau fédérateur jusqu'à ce qu'ils atteignent la zone générale de la destination.. À ce stade, ils se déplacent du dernier routeur de réseau fédérateur à un ou plusieurs routeurs hors du réseau fédérateur jusqu'à la destination finale.

Les systèmes de routage désignent souvent des groupes logiques de nœuds, appelés domaines, systèmes autonomes ou zones. Dans les systèmes hiérarchiques, certains routeurs d'un domaine peuvent communiquer avec les routeurs d'autres domaines, tandis que d'autres ne peuvent communiquer qu'avec les routeurs de leur domaine. Dans les très grands réseaux, il peut exister des niveaux hiérarchiques supplémentaires, les routeurs du niveau hiérarchique le plus élevé constituant le réseau fédérateur de routage.

Le principal avantage du routage hiérarchique est qu'il imite l'organisation de la plupart des entreprises et, par conséquent, prend bien en charge leurs schémas de trafic. La plupart des communications réseau se produisent au sein de petits groupes d'entreprise (domaines). Comme les routeurs intra-domaines n'ont besoin de connaître que les autres routeurs de leur domaine, leurs algorithmes de routage peuvent être simplifiés et, selon l'algorithme de routage utilisé, le trafic de mise à jour de routage peut être réduit en conséquence.

État de lien ou vecteur de distance

Les algorithmes d'état de liens (également appelés algorithmes du plus court chemin d'abord) acheminent les informations de routage à tous les nœuds de l'inter-réseau. Cependant, chaque routeur envoie uniquement la partie de la table de routage qui décrit l'état de ses propres liaisons. Dans les algorithmes à état de liens, chaque routeur construit une image de l'ensemble du réseau dans ses tables de routage. Les algorithmes de vecteurs de distance (également appelés algorithmes de Bellman-Ford) exigent que chaque routeur envoie la totalité ou une partie de sa table de routage, mais uniquement à ses voisins. En gros, les algorithmes à état de liens envoient de petites mises à jour partout, tandis que les algorithmes à vecteur de distance envoient des mises à jour plus volumineuses uniquement aux routeurs voisins. Les algorithmes de vecteurs de distance ne connaissent que leurs voisins. En règle générale, les algorithmes d'état de liaison sont utilisés conjointement avec les protocoles de routage OSPF.

Protocoles Internet pris en charge pour le routage

L'appareil de défense contre les menaces prend en charge plusieurs protocoles Internet pour le routage. Chaque protocole est décrit brièvement dans cette section.

- Protocole de routage de passerelle intérieure amélioré (EIGRP)

  EIGRP est un protocole exclusif de Cisco qui assure la compatibilité et une interopération transparente avec les routeurs IGRP. Un mécanisme de redistribution automatique permet aux routes IGRP d'être importées dans le protocole Enhanced IGRP, et inversement. Il est donc possible d'ajouter progressive-ment le protocole Enhanced IGRP à un réseau IGRP existant.

- Open Shortest Path First (OSPF)

  OSPF est un protocole de routage mis au point pour les réseaux IP (Internet Protocol) par le groupe de travail IGP (Interior Gateway Protocol) de l'Internet Engineering Task Force (IETF). OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF comprend une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

- Protocole RIP (Routing Information Protocol)

  IPS est un protocole de vecteur de distance qui utilise le nombre de sauts comme mesure. Il s'agit d'un protocole IGP (Interior Gateway Protocol), ce qui signifie qu'il effectue le routage au sein d'un seul système autonome.

- Protocole de routage BGP

  BGP est un protocole de routage de système inter autonome. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP). Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

Table de routage

Le défense contre les menaces utilise des tableaux de routage distincts pour le trafic de données (via le périphérique) et pour le trafic de gestion (du périphérique). Cette section décrit le fonctionnement des tables de routage. Pour en savoir plus sur la table de routage de gestion, consultez également Table de routage pour le trafic de gestion, à la page 14.

Mode de remplissage de la table de routage

La table de routage défense contre les menaces peut être remplie par des routes définies de manière statique, des routes connectées directement et des routes découvertes par les protocoles de routage dynamique. Comme le périphérique défense contre les menaces peut exécuter plusieurs protocoles de routage en plus d'avoir des routes statiques et connectées dans la table de routage, il est possible qu'une même route soit découverte ou saisie de plusieurs manières. Lorsque deux routes vers la même destination sont mises dans la table de routage, celle qui reste dans la table de routage est déterminée comme suit :

- Si les deux routes ont des longueurs de préfixe de réseau différentes (masques de réseau), les deux routes sont considérées comme uniques et sont entrées dans la table de routage. La logique de transfert de paquets détermine ensuite laquelle des deux utiliser.

  Par exemple, si les processus RIP et OSPF ont découvert les routes suivantes :

  - RIP : 192.168.32.0/24
  - OSPF : 192.168.32.0/19

  Même si les routes OSPF ont la meilleure distance administrative, les deux routes sont installées dans la table de routage, car chacune de ces routes a une longueur de préfixe différente (masque de sous-réseau). Ce sont des destinations considérées comme différentes et la logique de transfert de paquets détermine la route à utiliser.

- Si le périphérique défense contre les menaces connaît plusieurs chemins vers la même destination à partir d'un protocole de routage unique, comme RIP, la voie de routage avec la meilleure mesure (déterminée par le protocole de routage) est entrée dans la table de routage.

  Les métriques sont des valeurs associées à des routes spécifiques, de la plus préférée à la moins préférée. Les paramètres utilisés pour déterminer les métriques varient selon le protocole de routage. Le chemin avec la mesure la plus basse est sélectionné comme chemin optimale et installé dans la table de routage.

S’il existe plusieurs chemins vers la même destination avec des métriques égales, l’équilibrage de la charge est effectué sur ces chemins de coût égal.

- Si le périphérique défense contre les menaces connaît une destination à partir de plus d’un protocole de routage, les distance administratives des routages sont comparées et les routes avec une distance administrative inférieure sont entrées dans la table de routage.

Distances administratives pour les routages

Vous pouvez modifier les distance administratives pour les routages détectés ou redistribués dans un protocole de routage. Si deux routes de deux protocoles de routage différents ont la même distance administrative, la route avec la distance administrative *par défaut* la plus faible est entrée dans la table de routage. Dans le cas des routes EIGRP et OSPF, si la route EIGRP et la route OSPF ont la même distance administrative, la route EIGRP est choisie par défaut.

La distance administrative est un paramètre de routage que appareil de défense contre les menaces utilise pour sélectionner le meilleur chemin lorsqu'il existe deux ou plusieurs itinéraires différents vers la même destination à partir de deux protocoles de routage différents. Puisque les protocoles de routage ont des mesures basées sur des algorithmes différents des autres protocoles, il n’est pas toujours possible de déterminer le meilleur chemin pour deux routages vers la même destination qui ont été générées par différents protocoles de routage.

Chaque protocole de routage est priorisé à l’aide d’une valeur de distance administrative. Le tableau suivant présente les valeurs de distance administrative par défaut pour les protocoles de routage pris en charge par appareil de défense contre les menaces .

Tableau 1 : Distance administrative par défaut pour les protocoles de routage pris en charge

Source de la route	Distance administrative par défaut
Interface connectée	0
Routage VPN	1
Routage statique	1
Routage résumé EIGRP	5
BGP externe	20
EIGRP interne	90
OSPF	110
IS-IS	115
RIP	120
Routage EIGRP externe	170
BGP interne et local	200
Inconnu	255

Plus la valeur de la distance administrative est faible, plus la préférence est donnée au protocole. Par exemple, si l'appareil de défense contre les menaces reçoit une voie de routage vers un certain réseau d'un processus de routage OSPF (distance administrative par défaut - 110) et d'un processus de routage RIP (distance administrative par défaut - 120), l'appareil de défense contre les menaces choisit la voie de routage OSPF, car OSPF a une préférence plus élevée. Dans ce cas, le routeur ajoute la version OSPF de la route à la table de routage.

Une route VPN annoncée (V-Route/RRI) équivaut à une route statique avec la distance administrative par défaut de 1. Mais elle comporte une préférence plus élevée, comme avec le masque de réseau 255.255.255.255.

Dans cet exemple, si la source de routage dérivée OSPF était perdue (par exemple, en raison d'une coupure de courant), l'appareil de défense contre les menaces utiliserait alors le routage dérivé RIP jusqu'à ce que le routage dérivé OSPF réapparaisse.

La distance administrative est un paramètre local. Par exemple, si vous modifiez la distance administrative des routages obtenus par OSPF, cette modification n'affectera que la table de routage du appareil de défense contre les menaces pour lequel la commande a été saisie. La distance administrative n'est pas annoncée dans les mises à jour de routage.

La distance administrative n'affecte pas le processus de routage. Les processus de routage n'annoncent que les routages détectés par le processus de routage ou redistribués dans le processus de routage. Par exemple, le processus de routage RIP annonce les routes RIP, même si les routes découvertes par le processus de routage OSPF sont utilisées dans la table de routage.

Sauvegarde des routes dynamiques et statiques flottantes

Une route de secours est enregistrée lorsque la tentative initiale d'installation de la route dans la table de routage échoue parce qu'une autre route a été installée à la place. Si la voie de routage qui a été installée dans la table de routage échoue, le processus de maintenance de la table de routage appelle chaque processus de protocole de routage qui a enregistré une voie de routage de secours et lui demande de réinstaller la voie de routage dans la table de routage. S'il existe plusieurs protocoles avec des routes de secours enregistrées pour la voie de routage ayant échoué, la voie de routage préférée est choisie en fonction de la distance administrative.

Grâce à ce processus, vous pouvez créer des routes statiques flottantes qui sont installées dans la table de routage lorsque la route découverte par un protocole de routage dynamique échoue. Une voie de routage statique flottante est tout simplement une voie de routage statique configurée avec une distance administrative supérieure à celle des protocoles de routage dynamique s'exécutant sur appareil de défense contre les menaces . Lorsque la voie de routage correspondante découverte par un processus de routage dynamique échoue, la voie de routage statique est installée dans la table de routage.

Prise des décisions de transfert

Les décisions de transfert sont prises comme suit :

- Si la destination ne correspond à aucune entrée de la table de routage, le paquet est acheminé par l'intermédiaire de l'interface spécifiée pour la voie de routage par défaut. Si une voie de routage par défaut n'a pas été configurée, le paquet est rejeté.
- Si la destination correspond à une seule entrée dans la table de routage, le paquet est acheminé par l'interface associée à cette voie de routage.
- Si la destination correspond à plus d'une entrée dans la table de routage, le paquet est transféré hors de l'interface associée à la voie de routage qui a la plus grande longueur de préfixe de réseau.

Par exemple, un paquet destiné à 192.168.32.1 arrive sur une interface avec les routes suivantes dans la table de routage :

- Passerelle 192.168.32.0/24 10.1.1.2
- Passerelle 192.168.32.0/19 10.1.1.3

Dans ce cas, un paquet destiné à 192.168.32.1 est dirigé vers 10.1.1.2, car 192.168.32.1 fait partie du réseau 192.168.32.0/24. Il fait également partie de l'autre voie de routage dans la table de routage, mais 192.168.32.0/24 a le préfixe le plus long dans la table de routage (24 bits vers 19 bits). Les préfixes les plus longs sont toujours préférables aux plus courts lors du transfert d'un paquet.

Remarque Les connexions existantes continuent d'utiliser leurs interfaces établies même si une nouvelle connexion similaire entraînerait un comportement différent en raison d'une modification des routages.

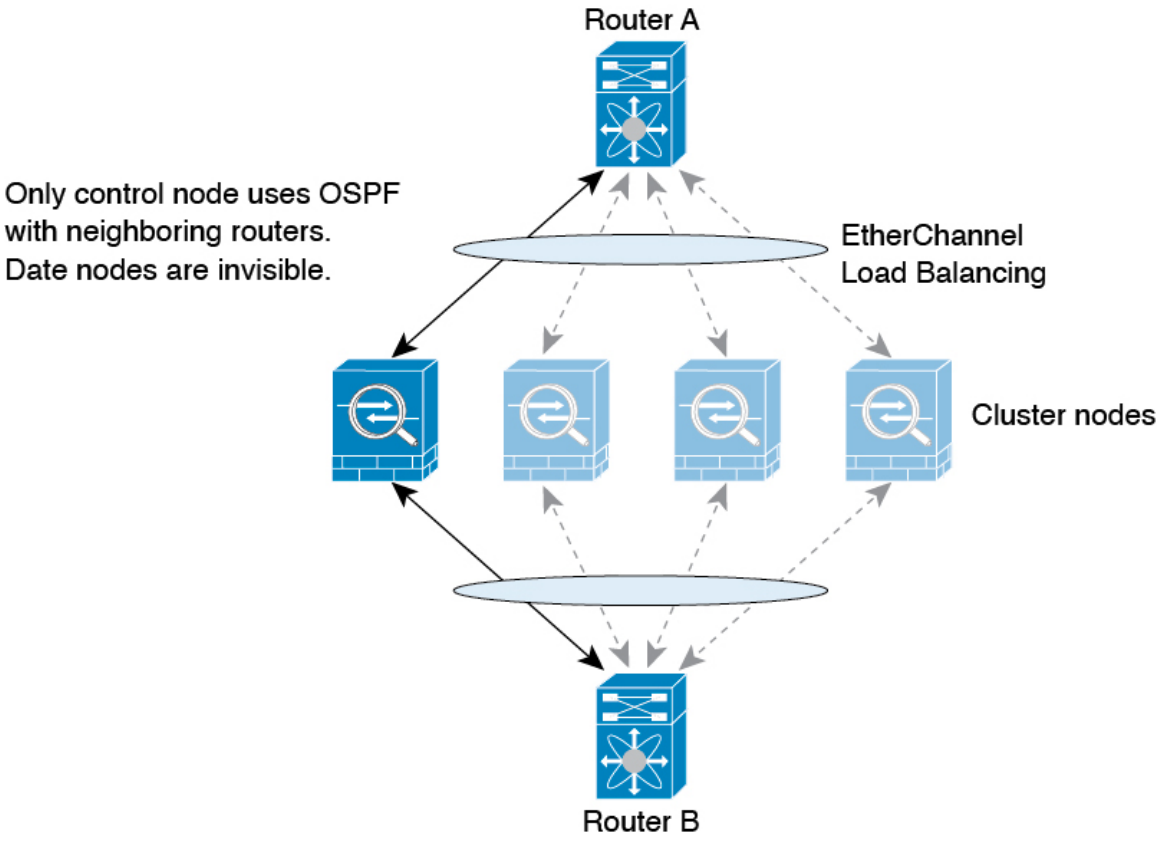
Routage dynamique et High Availability (haute disponibilité)

Les routages dynamiques sont synchronisés sur l'unité de secours lorsque la table de routage change sur l'unité active. Cela signifie que tous les ajouts, suppressions ou modifications effectués sur l'unité active sont immédiatement répercutés sur l'unité en veille. Si l'unité de secours devient active dans une paire actif/secours High Availability (haute disponibilité) prête, elle aura déjà une table de routage identique à celle de l'unité active précédente, car les routages sont synchronisés dans le cadre de la synchronisation en bloc High Availability (haute disponibilité) et des processus de duplication continue.

Routage dynamique en mode Mise en grappe)

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 1 : Routage dynamique en mode EtherChannel étendu



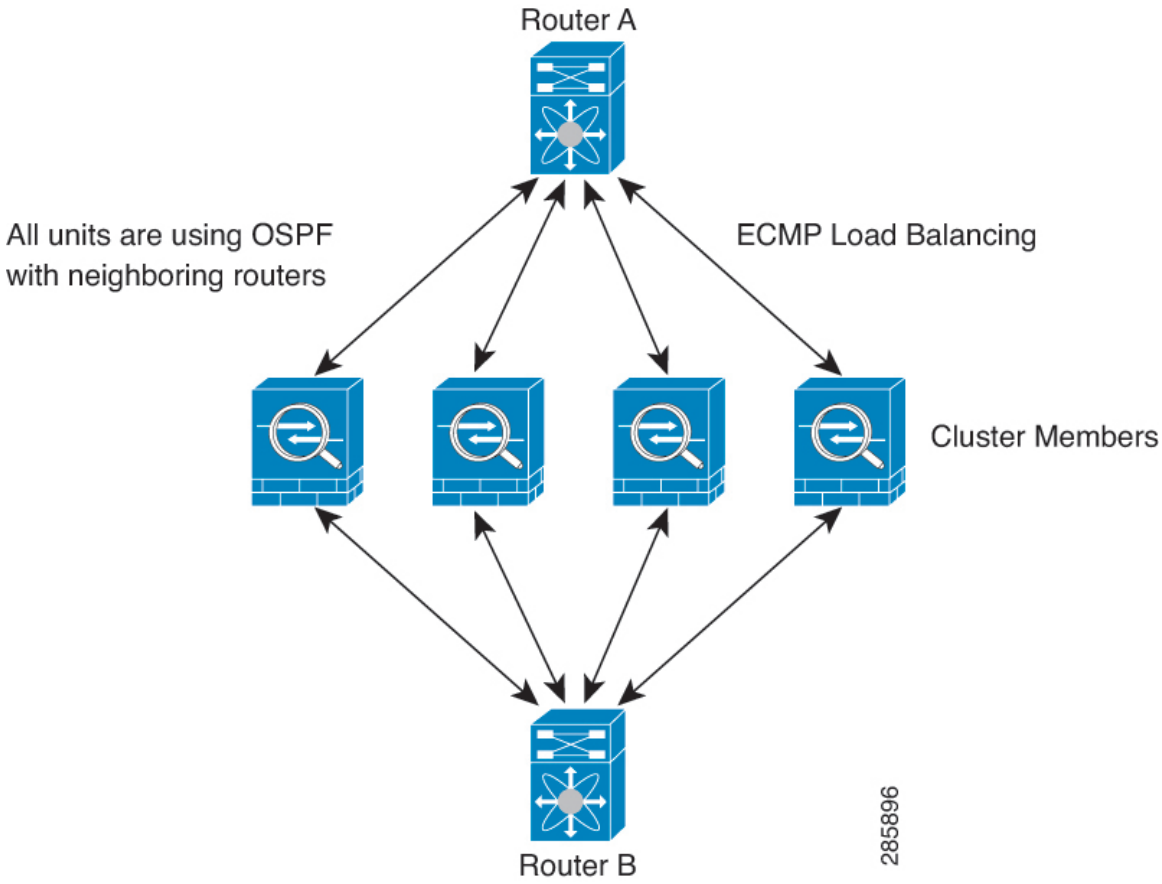
Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

Routage dynamique en mode d'interface individuelle

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 2 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Créer une zone ECMP.

Table de routage pour le trafic de gestion

En tant que pratique de sécurité courante, il est souvent nécessaire de séparer et d'isoler le trafic de gestion (provenant du périphérique) du trafic de données. Pour réaliser cet isolement, défense contre les menaces utilise une table de routage distincte pour le trafic de gestion uniquement par rapport au trafic de données.

Des tableaux de routage distincts signifient que vous pouvez créer des routages par défaut distincts pour les données et la gestion.

Types de trafic pour chaque table de routage

Le trafic de l'appareil utilise toujours la table de routage des données.

Le trafic en provenance du périphérique, selon le type, utilise par défaut la table de tourage réservé à la gestion ou la table de routage des données. Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

- Le trafic du tableau de gestion uniquement en provenance du périphérique comprend les communications du serveur AAA.
- Le trafic du tableau de données du périphérique comprend les recherches de serveur DNS et le DDNS. Une exception est que si vous spécifiez uniquement l'interface de diagnostic pour DNS, le défense contre les menaces utilisera uniquement le tableau de gestion uniquement.

Interfaces incluses dans la table de routage de gestion uniquement

Les interfaces de gestion uniquement comprennent toutes les interfaces x/x Diagnostic ainsi que toutes les interfaces que vous avez configurées pour être uniquement de gestion.

Remarque L'interface logique de gestion utilise sa propre table de routage Linux qui ne fait pas partie de la recherche de routage défense contre les menaces . Le trafic provenant de l'interface de gestion comprend la communicationcentre de gestion, la communication des licences et les mises à niveau de la base de données. L'interface logique de diagnostic, quant à elle, utilise la table de routage de gestion uniquement décrite dans cette section.

Repli vers l'autre table de routage

Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

Utilisation de la table de routage autre que par défaut

Si vous avez besoin que le trafic initial sorte d'une interface qui ne figure pas dans sa table de routage par défaut, vous devrez peut-être spécifier cette interface lorsque vous la configurerez, plutôt que de vous fier à l'autre table. Le périphérique défense contre les menaces vérifiera uniquement les routages de l'interface spécifiée. Par exemple, si vous devez communiquer avec un serveur RADIUS sur une interface de données, spécifiez cette interface dans la configuration RADIUS. Sinon, s'il existe une route par défaut dans la table de routage de gestion uniquement, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage des données.

Routage dynamique

La table de routage réservé à la gestion prend en charge le routage dynamique distinct du table de routage de l'interface de données. Un processus de routage dynamique donné doit s'exécuter sur l'interface de gestion uniquement ou sur l'interface de données; vous ne pouvez pas mélanger les deux types.

Routage à chemins multiples à coûts égaux (ECMP).

L'appareil de défense contre les menaces prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

ECMP sur plusieurs interfaces à l'aide de zones de trafic

Si vous configurez des zones de trafic pour contenir un groupe d'interfaces, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au sein de chaque zone. Par exemple, vous pouvez configurer plusieurs routes par défaut sur trois interfaces dans la zone :

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'appareil de défense contre les menaces équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, le périphérique déplace le flux de manière transparente vers une autre route.

À propos des cartes de routage

Les cartes de routage sont utilisées lors de la redistribution des routes dans un processus de routage OSPF, RIP, EIGRP ou BGP. Elles sont également utilisées lors de la génération d'une route par défaut dans un processus de routage. Une carte de routage définit les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible.

Les cartes de routage ont de nombreuses caractéristiques en commun avec les listes de contrôle d'accès bien connues. Voici quelques-unes des caractéristiques communes aux deux :

- Il s'agit d'une séquence ordonnée d'instructions individuelles, et chacune a un résultat d'autorisation ou de refus. L'évaluation d'une liste de contrôle d'accès ou d'une carte de routage comprend une analyse de liste, dans un ordre prédéterminé, et une évaluation des critères de chaque énoncé qui correspond. Une analyse de liste est abandonnée une fois que la première correspondance d'instruction est trouvée et qu'une action associée à la correspondance d'instruction est effectuée.
- Ce sont des mécanismes génériques. Les correspondances de critères et l'interprétation des correspondances sont dictées par la façon dont elles sont appliquées et par la fonctionnalité qui les utilise. Une carte de routage appliquée à différentes entités peut être interprétée différemment.

Voici quelques-unes des différences entre les cartes de routage et les listes de contrôle d'accès :

- Les cartes de routage sont plus flexibles que les listes de contrôle d'accès et peuvent vérifier les routages en fonction de critères que les listes de contrôle d'accès ne peuvent pas vérifier. Par exemple, une carte de routage peut vérifier si le type de routage est interne.
- Chaque liste de contrôle d'accès se termine par une instruction de refus implicite, par convention de conception. Si la fin d'une carte de routage est atteinte pendant les tentatives de mise en correspondance,

le résultat dépend de l'application spécifique de la carte de routage. Les cartes de routage appliquées à la *redistribution* se comportent de la même manière que les listes de contrôle d'accès : si la route ne correspond à aucune clause d'une carte de routage, la redistribution de la route est refusée, comme si la carte de routage contient une déclaration de refus à la fin.

Clauses d'autorisation et de refus

Les cartes de routage peuvent avoir des clauses d'autorisation et de refus. La clause deny rejette les correspondances de routage de la redistribution. Vous pouvez utiliser une liste de contrôle d'accès comme critère de correspondance dans la carte de routage. Étant donné que les listes de contrôle d'accès ont également des clauses d'autorisation et de refus, les règles suivantes s'appliquent lorsqu'un paquet correspond à la liste de contrôle d'accès :

- ACL permit + route map permit : les routes sont redistribuées.
- ACL permit + route map deny : les routes ne sont pas redistribuées.
- ACL deny + route map permit or deny : la clause route-map n'est pas mise en correspondance et la prochaine clause route-map est évaluée.

Valeurs de clause de correspondance et de définition

Chaque clause de carte de routage a deux types de valeurs :

- Une valeur de correspondance sélectionne les routages auxquels cette clause doit être appliquée.
- Une valeur définie modifie les renseignements qui seront redistribués dans le protocole cible.

Pour chaque voie de routage qui est redistribuée, le routeur évalue d'abord les critères de correspondance d'une clause de la carte de routage. Si les critères de correspondance sont réussis, la route est redistribuée ou rejetée comme l'exige la clause allow ou deny , et certains de ses attributs peuvent être modifiés par les valeurs définies à partir des commandes set . Si les critères de correspondance échouent, cette clause ne s'applique pas à la voie de routage et le logiciel procède à l'évaluation de la voie de routage en fonction de la clause suivante de la carte de routage. L'analyse de la carte de routage se poursuit jusqu'à ce qu'une clause correspondant à la route soit trouvée ou jusqu'à ce que la fin de la carte de routage soit atteinte.

Une correspondance ou une valeur définie dans chaque clause peut être manquée ou répétée plusieurs fois, si l'une de ces conditions est remplie :

- Si plusieurs entrées de correspondance sont présentes dans une clause, elles doivent toutes réussir pour une route donnée afin que cette route corresponde à la clause (c'est-à-dire que l'algorithme AND logique est appliqué pour plusieurs commandes de correspondance).
- Si une entrée de correspondance fait référence à plusieurs objets dans une seule entrée, l'un ou l'autre doit correspondre (l'algorithme OU logique est appliqué).
- En l'absence d'entrée de correspondance, toutes les routes correspondent à la clause.
- Si une entrée d'ensemble n'est pas présente dans une clause d'autorisation de carte de routage, la route est redistribuée sans modification de ses attributs actuels.

Remarque Ne configurez pas d'entrée d'ensemble dans une clause de refus de carte de routage, car la clause de refus interdit la redistribution de routage : il n'y a aucun renseignement à modifier.

Une clause de carte de routage sans entrée de correspondance ou d'ensemble effectue une action. Une clause d'autorisation vide permet une redistribution des routes restantes sans modification. Une clause de refus vide ne permet pas une redistribution d'autres routes (il s'agit de l'action par défaut si une carte de routage est complètement analysée, mais qu'aucune correspondance explicite n'est trouvée).

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.