

Aperçu du routage

Ce chapitre décrit le comportement du routage dans l'ASA.

- Détermination du chemin, à la page 1
- Types de routage pris en charge, à la page 2
- Protocoles Internet pris en charge pour le routage, à la page 3
- Table de routage, à la page 4
- Table de routage pour le trafic de gestion, à la page 11
- Routage à chemins multiples à coûts égaux (ECMP), à la page 12
- Désactiver les demandes ARP du mandataire, à la page 13
- Afficher la table de routage, à la page 13
- Historique de l'aperçu du routage, à la page 14

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.

Remarque Le routage symétrique est uniquement pris en charge pour le basculement actif/actif dans le mode de contexte multiple.

Types de routage pris en charge

Un routeur peut utiliser plusieurs types de routage. L'ASA 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'ASA 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).

- Intermediate System-to-Intermediate System (IS-IS)

  IS-IS est un protocole IGP (Interior Gateway Protocol) à état de liaison. Les protocoles à état de liaison se caractérisent par la propagation des informations nécessaires pour créer une carte complète de la connectivité du réseau sur chaque routeur participant. Cette carte est ensuite utilisée pour calculer le chemin le plus court vers les destinations.

Routage du trafic GRE

Dans ASA, le trafic d'encapsulation de routage générique (GRE) est géré à l'aide de flux bidirectionnels. Cela signifie que chaque session GRE est représentée par une seule entrée de flux qui gère le trafic entrant et sortant entre les points terminaux. Avec les flux bidirectionnels, une seule recherche de routage est effectuée et les deux directions sont mappées sur la même interface. Par conséquent, le système ne peut pas prendre de décisions de routage indépendantes pour chaque direction, ce qui peut entraîner un routage sous-optimal dans certains scénarios.

Table de routage

L'ASA 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 11.

Mode de remplissage de la table de routage

La table de routage ASA 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 ASA 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 ASA 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 ASA 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 ASA 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 ASA.

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

Source de la route	Distance administrative par défaut
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'ASA 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'ASA 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'ASA 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 de l'ASA 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 ASA. 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 Basculement

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 Basculement 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 Basculement et des processus de duplication continue.

Routage et mise en grappe dynamiques

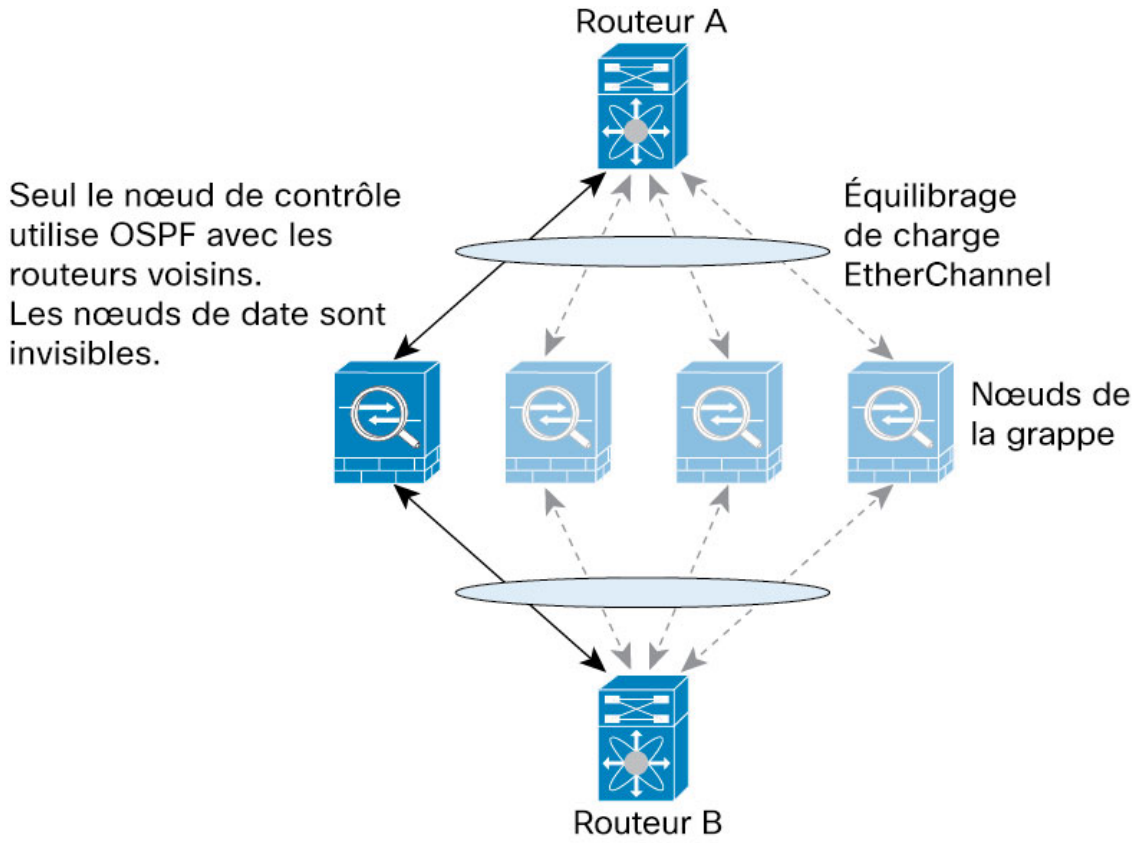
Cette section décrit comment utiliser le routage dynamique avec la mise en grappe.

Routage dynamique en mode EtherChannel étendu

Remarque IS-IS n'est pas pris en charge en mode EtherChannel étendu.

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



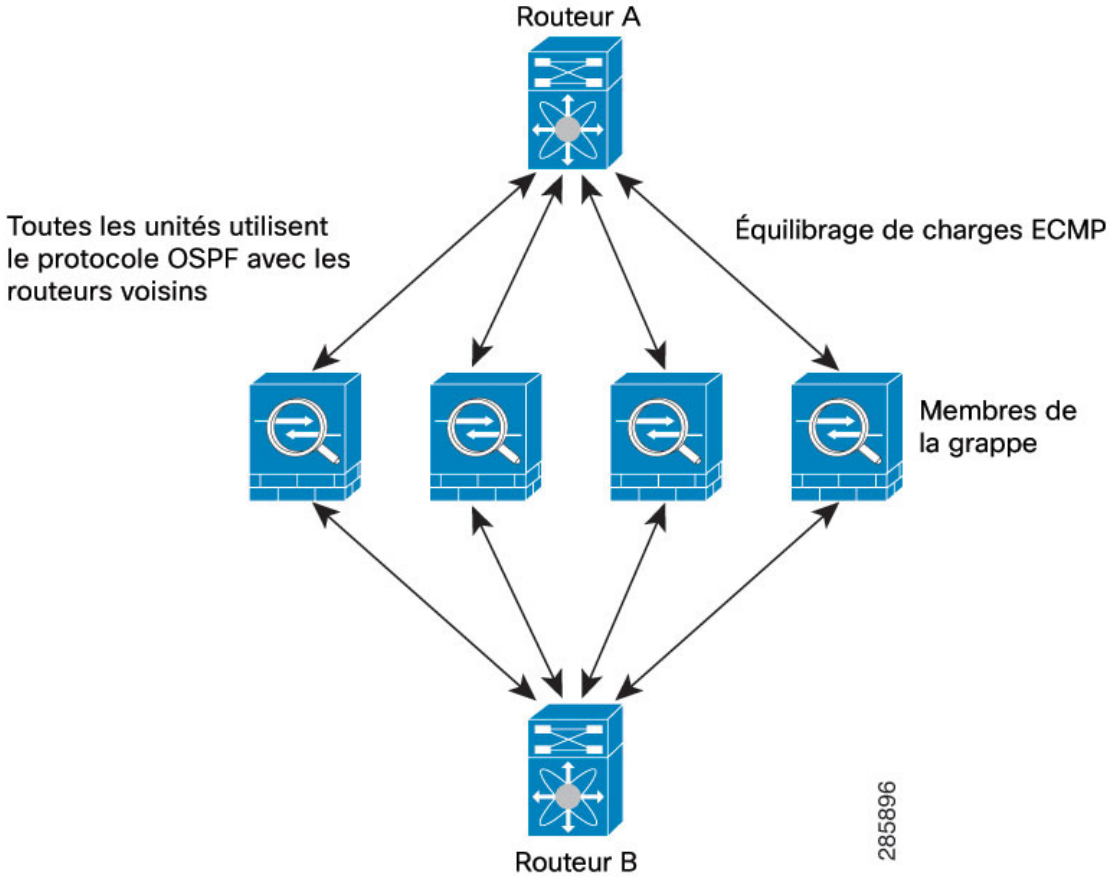
Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

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 Configurer une zone de trafic.

Routage dynamique en mode de contexte multiple

En mode de contexte multiple, chaque contexte gère une table de routage et des bases de données de protocole de routage distinctes. Cela vous permet de configurer les protocoles OSPFv2 et EIGRP indépendamment dans chaque contexte. Vous pouvez configurer le protocole EIGRP dans certains contextes et le protocole OSPFv2

dans le même contexte ou des contextes différents. En mode de contexte mixte, vous pouvez activer n'importe quel protocole de routage dynamique dans les contextes qui sont en mode routé. Les protocoles RIP et OSPFv3 ne sont pas pris en charge en mode de contexte multiple.

Le tableau suivant répertorie les attributs des protocoles EIGRP et OSPFv2, les cartes de routage utilisées pour la distribution des routes dans les processus OSPFv2 et EIGRP, ainsi que les listes de préfixes utilisées dans le protocole OSPFv2 pour filtrer les mises à jour de routage entrant ou sortant d'une zone lorsqu'elles sont utilisées en mode de contexte multiple :

EIGRP	OSPFv2	Cartes de routage et listes de préfixes
Une instance est prise en charge par contexte.	Deux instances sont prises en charge par contexte.	S. O.
Il est désactivé dans le contexte système.		S. O.
Deux contextes peuvent utiliser les mêmes numéros de système autonome ou des numéros différents.	Deux contextes peuvent utiliser des ID de zone identiques ou différents.	S. O.
Les interfaces partagées dans deux contextes peuvent avoir plusieurs instances EIGRP en cours d'exécution.	Les interfaces partagées dans deux contextes peuvent avoir plusieurs instances OSPF en cours d'exécution.	S. O.
L'interaction des instances EIGRP sur les interfaces partagées est prise en charge.	L'interaction des instances OSPFv2 sur les interfaces partagées est prise en charge.	S. O.
Toutes les interfaces de ligne de commande disponibles en mode unique le sont également en mode de contexte multiple.		
Chaque interface de ligne de commande n'a d'effet que dans le contexte dans lequel elle est utilisée.		

Gestion des ressources de routage

Une classe de ressources appelée *routes* spécifie le nombre maximum d'entrées de table de routage pouvant exister dans un contexte. Cela résout le problème d'un contexte affectant les entrées de table de routage disponibles dans un autre contexte et vous permet également de mieux contrôler le nombre maximum d'entrées de route par contexte.

Comme il n'y a pas de limite système définitive, vous pouvez uniquement spécifier une valeur absolue pour cette limite de ressource; vous ne pouvez pas utiliser de limite de pourcentage. De plus, il n'y a pas de limites minimum et maximum par contexte, de sorte que la classe par défaut ne change pas. Si vous ajoutez une nouvelle route pour l'un des protocoles de routage statique ou dynamique (connecté, statique, OSPF, EIGRP et RIP) dans un contexte et que la limite de ressources pour ce contexte est expirée, l'ajout de route échoue et un message de journal système est généré.

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, le périphérique ASA 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 de la table de gestion uniquement à partir de l'appareil comprend des fonctionnalités qui ouvrent un fichier distant à l'aide de HTTP, SCP, TFTP, la commande **copy** , les licences Smart, Smart Call Home, **trustpointtrustpool**, etc.
- Le trafic du tableau de données du périphérique comprend toutes les autres fonctionnalités telles que le ping, le DNS, le DHCP, etc.

Interfaces incluses dans la table de routage de gestion uniquement

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

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 ASA vérifiera uniquement les routes pour l'interface spécifiée. Par exemple, si vous avez besoin d'un ping pour sortir une interface de gestion uniquement, spécifiez l'interface dans la fonction envoyer un message Ping. Sinon, s'il existe une route par défaut dans la table de routage de données, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage de gestion.

Routage dynamique

La table de routage réservé à la gestion prend en charge le routage dynamique distinct de la 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. Lors de la mise à niveau à partir d'une version antérieure sans table de routage de gestion distinct, si vous avez un mélange d'interfaces de données et de gestion utilisant le même processus de routage dynamique, les interfaces de gestion seront abandonnées.

Fonctionnalité d'accès de gestion pour les exigences VPN

Si vous configurez la fonctionnalité d'accès de gestion qui permet l'accès de gestion à une interface autre que celle à partir de laquelle vous avez entré l'ASA lors de l'utilisation du VPN, alors, en raison de considérations de routage avec les tables de gestion et de routage de données distinctes, l'interface de terminaison VPN et la gestion L'interface d'accès doit être du même type : les deux doivent être des interfaces de gestion uniquement ou des interfaces de données standard.

Identification de l'interface de gestion

Une interface configurée avec l'option de gestion uniquement est considérée comme une interface de gestion.

Dans la configuration suivante, les interfaces GigabitEthernet0/0 et Management0/0 sont considérées comme des interfaces de gestion.

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

Routage à chemins multiples à coûts égaux (ECMP)

L'ASA 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'ASA 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.

Désactiver les demandes ARP du mandataire

Lorsqu'un hôte envoie du trafic IP à un autre périphérique sur le même réseau Ethernet, l'hôte doit connaître l'adresse MAC du périphérique. ARP est un protocole de couche 2 qui résout une adresse IP en une adresse MAC. Un hôte envoie une demande ARP de type « À qui appartient cette adresse IP? ». Le périphérique qui possède l'adresse IP répond : « Je possède cette adresse IP; voici mon adresse MAC. »

L'ARP du mandataire est utilisé lorsqu'un périphérique répond à une demande ARP avec sa propre adresse MAC, même si le périphérique ne possède pas l'adresse IP. L'ASA utilise un ARP de mandataire lorsque vous configurez la NAT et spécifiez une adresse mappée qui se trouve sur le même réseau que l'interface ASA. Le trafic ne peut atteindre les hôtes que si l'ASA utilise un ARP de mandataire pour revendiquer que l'adresse MAC est attribuée aux adresses mappées de destination.

Dans de rares cas, vous souhaiterez peut-être désactiver l'ARP du mandataire pour les adresses NAT.

Si vous avez un ensemble d'adresses du client VPN qui chevauche un réseau existant, l'ASA envoie par défaut des demandes ARP de mandataire sur toutes les interfaces. Si vous avez une autre interface qui se trouve sur le même domaine de couche 2, elle verra les demandes ARP et répondra par l'adresse MAC de son interface. Il en résulte que le trafic de retour des clients VPN vers les hôtes internes ira à la mauvaise interface et sera abandonné. Dans ce cas, vous devez désactiver les demandes ARP de mandataire pour l'interface sur laquelle vous ne les souhaitez pas.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Proxy ARP/Neighbor Discovery (ARP de mandataire/Découverte de voisin)**.

Le champ Interface répertorie les noms d'interface. Le champ Enabled (Activé) indique si l'option ARP de mandataire/découverte de voisin est activée (Oui) ou désactivée (Non) pour les adresses globales NAT.

Étape 2 Pour activer l'option ARP de mandataire/découverte de voisin pour l'interface sélectionnée, cliquez sur **Enable** (Activer). Par défaut, l'option ARP de mandataire/découverte de voisin est activée pour toutes les interfaces.

Étape 3 Pour désactiver l'option ARP de mandataire/découverte de voisin pour l'interface sélectionnée, cliquez sur **Disable** (Désactiver).

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer vos paramètres dans la configuration d'exécution.

Afficher la table de routage

Pour afficher toutes les routes d'ASDM qui se trouvent dans la table de routage, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **Routes**. Chaque ligne représente une route.

Historique de l'aperçu du routage

Tableau 2 : Historique de l'aperçu du routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Table de routage pour l'interface de gestion	9.5(1)	Pour séparer et isoler le trafic de gestion du trafic de données, une table de routage distincte est ajoutée pour le trafic de gestion. Des tables de routage distinctes, pour la gestion et les données respectivement, sont créées pour IPv4 et IPv6, pour chaque contexte, de l'ASA. De plus, pour chaque contexte de l'ASA, deux tables de routage supplémentaires sont ajoutées dans la RIB et la FIB. Nous avons mis à jour les écrans suivants :

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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

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.