

BGP

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de passerelle frontière (BGP).

- BGP, à la page 1
- Lignes directrices BGP, à la page 5
- Configurer le protocole BGP, à la page 6
- Supervision BGP, à la page 28
- Historique de BGP, à la page 29

BGP

Le protocole de passerelle frontière (BGP) est un protocole de routage inter et intra-systèmes autonomes qui

- fonctionne au sein des systèmes autonomes et entre ceux-ci (réseaux ou groupes de réseaux soumis à une administration et à des politiques de routage communes),
- échange des informations de routage pour Internet, et
- sert de protocole entre les fournisseurs de services Internet (FSI).

Scénarios d'utilisation de BGP

Les scénarios d'utilisation de BGP sont des configurations réseau qui

- permettent aux fournisseurs de services Internet d'échanger des routes client et ISP entre des systèmes autonomes à l'aide d'un BGP externe (EBGP),
- permettent aux fournisseurs de services d'échanger des routes au sein d'un système autonome utilisant le BGP intérieur (IBGP), et
- prennent en charge le routage de préfixe IPv6 sur les réseaux IPv6.

Contextes de mise en œuvre de BGP

Les réseaux des clients, comme les universitaires et les entreprises, emploient généralement un protocole IGP (Interior Gateway Protocol) comme OSPF pour l'échange d'informations de routage au sein de leurs réseaux. 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).

BGP peut également être utilisé pour acheminer des informations de routage pour le préfixe IPv6 sur les réseaux IPv6.



Remarque Lorsqu'un périphérique BGPv6 rejoint la grappe, il génère un traçage logiciel lorsque le niveau de journalisation 7 est activé.

Modifications apportées à la table de routage

Les modifications de tableau de routage sont des mises à jour de réseau qui

- se produisent lorsque les voisins BGP échangent des informations de routage complètes lors de l'établissement initial de la connexion TCP
- impliquent l'envoi uniquement des routes modifiées aux voisins lorsque des modifications de table de routage sont détectées, et
- annoncent uniquement le CHEMIN optimal vers un réseau de destination sans mises à jour périodiques.

Attributs BGP pour la sélection de la voie de routage

Les voies de routage apprises via BGP ont des propriétés utilisées pour déterminer la meilleure voie de routage lorsque plusieurs chemins vers une destination existent. Ces propriétés sont appelées attributs BGP et sont utilisées dans le processus de sélection de la voie de routage :

- Pondération : il s'agit d'un attribut défini par Cisco qui est local à un routeur. L'attribut de pondération n'est pas annoncé aux routeurs voisins. Si le routeur détecte l'existence de plusieurs routes vers la même destination, la route ayant la pondération la plus élevée est préférée.
- Préférence locale : l'attribut de préférence locale est utilisé pour sélectionner un point de sortie du système autonome local. Contrairement à l'attribut de poids, il est partagé dans l'ensemble du système autonome local. S'il y a plusieurs points de sortie, celui dont l'attribut de préférence locale est le plus élevé est choisi pour une voie de routage spécifique.
- Identifiant multi-sortie : L'attribut de métrique ou de discrimination multi-sortie (MED) est utilisé comme suggestions à un système autonome externe concernant la voie de routage préférée dans le système autonome qui annonce la métrique. Il s'agit d'une suggestions, car le système autonome externe qui reçoit les MED peut également utiliser d'autres attributs de BGP pour la sélection de route. La route avec la métrique MED la plus basse est préférée.
- Origine : l'attribut d'origine indique comment BGP a appris l'existence d'une route particulière. L'attribut d'origine peut avoir l'une des trois valeurs possibles et est utilisé dans la sélection de la route.
  - IGP : la voie de routage est intérieure au système autonome d'origine. Cette valeur est définie lorsque la commande de configuration du routeur network est utilisée pour injecter la voie de routage dans BGP.
  - EGP : le routage est appris par le protocole EBGP (Exterior Border Gateway Protocol).

- Incomplet : l’origine de la route est inconnue ou apprise d’une autre manière. Une origine incomplète se produit lorsqu'une route est redistribuée dans BGP.

- AS_path : lorsqu’une déclaration de route passe par un système autonome, le numéro de système autonome est ajouté à une liste ordonnée de numéros de système autonome que l’annonce de route a traversés. Seule la voie de routage avec la liste AS_path la plus courte est installée dans la table de routage IP.
- Saut suivant : l'attribut de saut suivant EBGP est l'adresse IP utilisée pour atteindre le routeur publicitaire. Pour les homologues EBGP, l’adresse de saut suivant est l’adresse IP de la connexion entre les homologues. Pour IBGP, l’adresse du prochain saut EBGP est acheminée dans le système autonome local. Cependant, lorsque le saut suivant se trouve dans le même sous-réseau que l’adresse d’appairage de l’homologue eBGP, le saut suivant n’est pas modifié. Ce comportement est appelé saut suivant du tiers.

  Utilisez la commande **next-hop-self** lors de la redistribution des routes annoncées par VPN vers les homologues iBGP pour vous assurer que les routes sont redistribuées avec l’adresse IP du prochain saut appropriée.
- Community (Communauté) : l’attribut Community permet de regrouper des destinations, appelées communautés, auxquelles les décisions de routage (telles que l’acceptation, les préférences et la redistribution) peuvent être appliquées. Des cartes de routage sont utilisées pour définir l’attribut de communauté. Les attributs de communauté prédéfinis sont les suivants :
  - no-export : n’annonce pas cette voie de routage aux homologues EBGP.
  - no-advertise : n’annonce cette voie de routage à aucun homologue.
  - Internet : annonce cette route à la communauté Internet; tous les routeurs du réseau lui appartiennent.



Remarque La détection de boucle AS se fait en analysant le chemin AS complet (comme spécifié dans l’attribut AS_PATH) et en vérifiant que le numéro de système autonome du système local ne figure pas dans le chemin AS. Par défaut, EBGP annonce les routes apprises au même homologue pour éviter des cycles de CPU supplémentaires sur la périphérique lors des vérifications de boucle et des retards dans les tâches de mise à jour sortantes existantes.

Sélection du chemin BGP

La sélection de chemin BGP est un processus de routage qui sélectionne un seul chemin comme meilleur chemin lorsque BGP reçoit plusieurs annonces pour la même voie de routage de différentes sources, place le chemin sélectionné dans la table de routage IP et propage le chemin à ses voisins à l’aide de critères spécifiques dans l’ordre de priorité.

Critères de sélection du chemin BGP

BGP utilise les critères suivants, dans l’ordre présenté, pour sélectionner un chemin pour une destination :

1. Si le chemin précise un saut suivant inaccessible, supprimez la mise à jour. Privilégiez le chemin avec la pondération la plus élevée.

2. Si les pondérations sont identiques, préférez le chemin avec la préférence locale la plus élevée. Si les préférences locales sont les mêmes, le chemin préféré est celui qui a été créé par le protocole BGP exécuté sur ce routeur.
3. Si aucune voie de routage n'a été créée, privilégiez la voie de routage qui a le chemin AS_path le plus court. Si tous les chemins ont la même longueur AS_path, privilégiez le chemin avec le type d'origine le plus bas (où IGP est inférieur à EGP et EGP est inférieur à incomplet).
4. Si les codes d'origine sont les mêmes, privilégiez le chemin avec l'attribut MED le plus bas. Si les chemins ont la même MED, privilégiez le chemin externe au chemin interne.
5. Si les chemins sont toujours les mêmes, privilégiez le chemin par le voisin IGP le plus proche. Déterminez si plusieurs chemins d'accès nécessitent l'installation dans la table de routage pour Chemins multiples BGP, à la page 4.
6. Déterminez si plusieurs chemins d'accès nécessitent l'installation dans la table de routage pour Chemins multiples BGP, à la page 4.
7. Si les deux chemins sont externes, privilégiez le chemin qui a été reçu en premier (le plus ancien).
8. Privilégiez le chemin avec l'adresse IP la plus basse, comme spécifié par l'ID du routeur BGP. Si l'ID de l'expéditeur ou du routeur est le même pour plusieurs chemins, privilégiez le chemin avec la longueur minimale de la liste de grappes.
9. Privilégiez le chemin qui provient de l'adresse du voisin le plus bas.

Chemins multiples BGP

Les chemins multiples BGP sont une fonctionnalité BGP qui

- permet l'installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination,
- permet de répartir le trafic vers le préfixe de destination sur tous les chemins installés, et
- n'affecte pas l'algorithme de sélection du meilleur chemin.

Exigences relatives aux chemins multiples BGP

Ces chemins sont installés dans le tableau avec le meilleur chemin pour le partage de la charge. Les chemins multiples BGP n'affectent pas la sélection du meilleur chemin. Par exemple, un routeur désigne toujours l'un des chemins comme le meilleur chemin, selon l'algorithme, et annonce ce meilleur chemin à ses homologues de BGP.

Pour être candidats aux chemins multiples, les chemins vers la même destination doivent présenter les mêmes caractéristiques que le meilleur chemin :

- Poids
- Préférence locale
- Longueur du chemin d'accès AS
- Code d'origine
- Sélecteur de sorties multiples (MED)

- L'une des suivantes :
  - Le système autonome ou sous-système autonome voisin (avant l'ajout des chemins multiples de BGP)
  - AS-PATH (après l'ajout des chemins multiples BGP)

Certaines fonctionnalités de chemins multiples BGP imposent des exigences supplémentaires aux chemins candidats :

- Le chemin doit être appris d'un voisin externe ou d'un voisin externe à la confédération (eBGP).
- La métrique IGP jusqu'au saut suivant BGP doit être égale à la métrique IGP du meilleur chemin.

Voici les exigences supplémentaires pour les candidats aux chemins multiples de BGP interne (iBGP) :

- Le chemin doit être appris d'un voisin interne (iBGP).
- La métrique IGP jusqu'au saut suivant BGP doit être égale à la métrique IGP du meilleur chemin, sauf si le routeur est configuré pour les chemins multiples iBGP à coût inégal.

BGP insère dans la table de routage IP jusqu'aux *n* chemins les plus récemment reçus parmi les chemins candidats, où *n* correspond au nombre de routes à installer dans la table de routage, comme indiqué lors de la configuration des chemins multiples BGP. La valeur par défaut, lorsque les chemins multiples est désactivé, est 1.

Pour l'équilibrage de charge à coût inégal, vous pouvez également utiliser la bande passante du lien BGP.

Remarque L'équivalent de next-hop-self est appliqué au meilleur chemin sélectionné parmi les chemins multiples eBGP avant son transfert aux homologues internes.

Lignes directrices BGP

Lignes directrices relatives au mode contextuel

Tenez compte de ces exigences en mode contexte lors de la mise en œuvre de BGP.

- Pris en charge en mode contexte unique et multiple.
- Un seul numéro du système autonome (AS) est pris en charge pour tous les contextes.

Lignes directrices sur le mode pare-feu

Le mode pare-feu transparent n'est pas pris en charge. BGP est pris en charge uniquement en mode routé.

Lignes directrices IPv6

Prend en charge IPv6.

Lignes directrices supplémentaires

Tenez compte de ces exigences et limites opérationnelles supplémentaires.

- Le système n'ajoute pas d'entrée de routage pour l'adresse IP reçue sur PPPoE dans la table de routage du CP. BGP recherche toujours dans la table de routage du CP le lancement de la session TCP. Par conséquent, BGP ne forme pas de session TCP.

  C'est pourquoi, BGP sur PPPoE n'est pas pris en charge.

- BGP n’est pas pris en charge sur les interfaces BVI ou de gestion uniquement.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- BGP avec PATH MTU (PMTU) peut entraîner des fluctuations de contiguïté en cas d’échec de la découverte de la MTU, en particulier avec le routage ECMP. Par conséquent, soyez prudent lorsque vous utilisez BGP, PMTU et ECMP, car des abandons de paquets peuvent se produire si la découverte de la MTU échoue pour une raison quelconque.
- La table BGP de l’unité membre n’est pas synchronisée avec la table de l’unité de contrôle. Seule sa table de routage est synchronisée avec celle de l’unité de contrôle.
- Activez la fonctionnalité de délai d’expiration progressif lorsque vous utilisez BGP sur les périphériques Firewall Threat Defense configurés en mode de haute accessibilité. L’activation de cette fonctionnalité réduit les abandons de paquets qui se produisent en raison de problèmes liés à la convergence de BGP.

Configurer le protocole BGP

Cette section décrit comment activer et configurer le processus BGP sur votre système.

Procédure

Étape 1 Activer BGP, à la page 6.
Étape 2 Définir le meilleur chemin pour un processus de routage BGP, à la page 8.
Étape 3 Configurer les listes de politiques, à la page 9.
Étape 4 Configurer les filtres de chemin AS, à la page 10.
Étape 5 Configurer les règles de communauté, à la page 11.
Étape 6 Configurer les paramètres de la famille d’adresses IPv4, à la page 12.
Étape 7 Configurer les paramètres de la famille d’adresses IPv6, à la page 20.

Activer BGP

Cette section décrit les étapes requises pour activer le routage BGP, établir un processus de routage BGP et configurer les paramètres BGP généraux.

Procédure

Étape 1 Pour le mode unique, dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **General (Général)**.



Remarque Pour le multimode, dans ASDM, choisissez Configuration > Context Management (Gestion de contextes) > BGP. Après avoir activé BGP, passez à un contexte de sécurité et activez BGP en choisissant **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > General (Général)**.

Étape 2 Cochez la case **Enable BGP Routing** (Activer le routage BGP).

Étape 3 Dans le champ AS Number (numéro de système autonome), saisissez le numéro de système autonome (AS) pour le processus BGP. Le numéro de système autonome comprend plusieurs numéros autonomes en interne. Le numéro AS peut être compris entre 1 et 4294967295 ou entre 1.0 et XX.YY.

Étape 4 (Facultatif) Cochez la case **Limit the number of AS numbers in the AS_PATH attribute of received routes** (Limiter le nombre de numéros du système autonome dans l'attribut AS_PATH des routes reçues) pour restreindre le nombre de numéros du système autonome dans l'attribut AS_PATH à un nombre précis. Les valeurs valides sont comprises entre 1 et 254.

Étape 5 (Facultatif) Cochez la case Log neighbor changes (Consigner les modifications des voisins) pour activer la journalisation des modifications du voisin de BGP (actives ou différées) et des réinitialisations. Cela aide à résoudre les problèmes de connectivité du réseau et à mesurer la stabilité du réseau.

Étape 6 (Facultatif) Cochez la case Use TCP path MTU discovery (Utiliser la découverte de la MTU de chemin TCP) pour utiliser la technique de découverte de la MTU du chemin afin de déterminer la taille maximale de l'unité de transmission (MTU) sur le chemin réseau entre deux hôtes IP. Cela permet d'éviter la fragmentation IP.

Étape 7 (Facultatif) Cochez la case Enable fast external failover (Activer le basculement externe rapide) pour réinitialiser la session de BGP externe immédiatement en cas de défaillance de la liaison.

Étape 8 (Facultatif) Cochez la case Enforce that first AS is peer's AS for EBGP Routes (Veiller à ce que le premier AS soit l'AS de l'homologue pour les routes EBGP) pour ignorer les mises à jour entrantes reçues d'homologues de BGP externes qui n'indiquent pas leur numéro de système autonome comme premier segment dans l'attribut AS_PATH. Cela empêche un homologue mal configuré ou non autorisé d'acheminer le trafic en affichant un routage comme s'il provenait d'un autre système autonome.

Étape 9 (Facultatif) Cochez la case Use dot notation for AS numbers (Utiliser la notation par point pour les numéros d'AS) afin de scinder le numéro AS complet de 4 octets binaires en deux mots de 16 bits chacun, séparés par un point. Les numéros AS de 0 à 65 553 sont représentés sous forme de nombres décimaux et les nombres AS supérieurs à 65 535 sont représentés à l'aide de la notation par point.

Étape 10 Fournissez les renseignements sur la minuterie dans la zone Neighbor timers (Minuteries de voisin) :

a) Dans le champ Keepalive interval (Intervalle Keepalive), saisissez l'intervalle de temps pendant lequel le voisin de BGP reste actif après n'avoir pas envoyé de message keepalive. À la fin de cet intervalle de maintien, l'homologue de BGP est déclaré mort si aucun message n'est envoyé. La valeur par défaut est 60 secondes.

b) Dans le champ Hold Time (Délai de rétention), saisissez l'intervalle de temps pendant lequel le voisin de BGP reste actif pendant qu'une connexion BGP est lancée et configurée. Les valeurs par défaut sont de 180 secondes.

c) (Facultatif) Dans le champ Min. Hold Time (Délai de rétention min.), saisissez l'intervalle de temps minimal pendant lequel le voisin de BGP reste actif pendant qu'une connexion BGP est lancée et configurée. Spécifiez une valeur comprise entre 0 et 65 535.

Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 11 (Facultatif) Dans la section Non Stop Forwarding (Transfert continu), procédez comme suit :

a) Cochez la case Enable Graceful Restart (Activer le redémarrage progressif) pour permettre aux homologues de l'ASA d'éviter une oscillation de routage à la suite d'un basculement.

b) Dans le champ Restart Time (Heure de redémarrage), précisez la durée pendant laquelle les homologues de l'ASA attendront pour supprimer les routes périmées avant qu'un message d'ouverture de BGP ne soit reçu. La valeur par défaut est 120secondes. Les valeurs valides sont comprises entre 1 et 3600.

c) Dans le champ Stale Path Time (Temps de parcours), saisissez la durée pendant laquelle l'ASA attendra avant de supprimer des routes périmées après la réception d'un message de fin d'enregistrement (EOR) de la part de l'ASA, qui redémarrera. La valeur par défaut est 360 secondes. Les valeurs valides sont comprises entre 1 et 3600.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Apply** (Appliquer).

Définir le meilleur chemin pour un processus de routage BGP

Cette section décrit les étapes requises pour configurer le meilleur chemin BGP. Pour en savoir plus sur le meilleur chemin, consultez Sélection du chemin BGP, à la page 3.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **Best Path (Meilleur chemin)**.

Le volet de configuration Best Path (Meilleur chemin) apparaît.

Étape 2 Dans le champ Default Local Preference (Préférence locale par défaut) spécifiez une valeur comprise entre 0 et 4294967295. La valeur par défaut est 100. Des valeurs plus élevées indiquent une préférence plus élevée. Cette préférence est envoyée à tous les routeurs et serveurs d'accès du système autonome local.

Étape 3 Cochez la case Allow comparing MED from different neighbors (Permet de comparer les MED de différents voisins) pour autoriser la comparaison du Discriminateur multi-sortie (MED) pour les chemins de voisins dans différents systèmes autonomes.

Étape 4 Cochez la case Compare router-id for identical EBGP paths (Comparer l'ID du routeur pour des chemins EBGP identiques) pour comparer les chemins similaires reçus d'homologues externes de BGP pendant le processus de sélection du meilleur chemin et faire passer le meilleur chemin à la route ayant le plus petit ID de routeur.

Étape 5 Cochez la case Pick the best MED path among paths advertised from the neighboring AS (Choisir le meilleur chemin MED parmi les chemins annoncés par l'AS voisin) pour activer la comparaison MED parmi les

chemins appris des homologues de la confédération. Ajoutez une nouvelle entrée réseau. La comparaison entre les MED est effectuée uniquement s'il n'y a aucun système autonome externe sur le chemin.

Étape 6 Cochez la case Treat missing MED as the least preferred one (Traiter le MED manquant comme le moins préféré) pour considérer l'attribut MED manquant comme ayant une valeur infinie, faisant de ce chemin le moins souhaitable; par conséquent, un chemin pour lequel un MED manquant est défaillant est préférable.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur Apply (appliquer).

Configurer les listes de politiques

Lorsqu'une liste de stratégie est référencée dans une carte de routage, toutes les déclarations de correspondance dans la liste de stratégie sont évaluées et traitées. Deux listes de politiques ou plus peuvent être configurées avec une carte de routage. Une liste de politiques peut également coexister avec d'autres instructions de mise en correspondance et d'ensemble préexistantes configurées dans la même carte de routage, mais en dehors de la liste de politiques. Cette section décrit les étapes requises pour configurer les listes de politiques.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **Policy Lists (Listes de politiques)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue Add Policy List (Ajouter une liste de politiques) s'affiche. À partir de cette boîte de dialogue, vous pouvez ajouter un nom de liste de politiques, son accès à la redistribution (c'est-à-dire autoriser ou refuser), faire correspondre des interfaces, spécifier des adresses IP, faire correspondre le chemin AS, faire correspondre la liste des noms de communauté, faire correspondre les mesures et faire correspondre les numéros de balise.

Étape 3 Dans le champ **Policy List Name**(Nom de la liste de politiques), entrez un nom unique pour la liste de politiques.

Étape 4 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 5 Cochez la case **Match Interfaces** (Correspondance des interfaces) pour distribuer les routes dont le prochain saut se trouve hors de l'une des interfaces spécifiées, puis effectuez l'une des opérations suivantes :

- Dans le champ **Interface**, saisissez le nom de l'interface.
- Dans le champ Interface, cliquez sur les points de suspension pour rechercher manuellement et localiser l'interface. Choisissez une ou plusieurs interfaces, cliquez sur **Interface**, puis cliquez sur **OK**.

Étape 6 Dans la zone Specify IP (Spécifier l'adresse IP), configurez les éléments suivants :

a) Cochez la case Match Address (Correspondance des adresses) pour redistribuer toutes les routes dont l'adresse réseau de destination est autorisée par une liste d'accès standard ou une liste de préfixes, et effectuez le routage des politiques sur les paquets.

Spécifiez une liste d'accès ou une liste de préfixes ou cliquez sur les points de suspension pour rechercher manuellement et localiser une liste d'accès. Choisissez une ou plusieurs listes d'accès, cliquez sur Access List (Liste d'accès), puis cliquez sur OK.

b) Cochez la case Match Next Hop (Correspondance des sauts suivants) pour redistribuer toutes les routes dont l'adresse du routeur de saut suivant est transmise par l'une des listes d'accès ou listes de préfixes spécifiées.

Spécifiez une liste d'accès/liste de préfixes ou cliquez sur les points de suspension pour rechercher manuellement et localiser une liste d'accès. Choisissez une ou plusieurs listes d'accès, cliquez sur Access List (Liste d'accès), puis cliquez sur OK.

c) Cochez la case Match Route Source (Correspondance source de route) pour redistribuer les routes qui ont été annoncées par les routeurs et les serveurs d'accès à l'adresse spécifiée par les listes d'accès ou la liste de préfixes.

Spécifiez une liste d'accès/liste de préfixes ou cliquez sur les points de suspension pour rechercher manuellement et localiser une liste d'accès. Choisissez une ou plusieurs listes d'accès, cliquez sur Access List (Liste d'accès), puis cliquez sur OK.

Étape 7 Cochez la case Match AS Path (Correspondance du chemin AS) pour faire correspondre un chemin de système autonome BGP.

Spécifiez un filtre de chemin AS ou cliquez sur les points de suspension pour rechercher manuellement et localiser le filtre de chemin AS. Choisissez un ou plusieurs filtres de chemin AS, cliquez sur AS Path Filter (Filtre de chemin AS), puis sur OK.

Étape 8 Cochez la case Match Community Names List (Associer la liste de noms de communauté) pour faire correspondre une communauté BGP.

a) Spécifiez une règle de communauté ou cliquez sur les points de suspension pour rechercher manuellement et localiser les règles de communauté. Sélectionnez une ou plusieurs règles de communauté, cliquez sur Community Rules (Règles de communauté), puis sur OK.
b) Cochez la case Match the specified community exactly (Faire correspondre exactement la communauté spécifiée) pour faire correspondre une communauté BGP spécifique.

Étape 9 Cochez la case **Match Metrices** (Correspondance des mesures) pour redistribuer les routes avec la mesure spécifiée. Si vous spécifiez plusieurs mesures, les routes peuvent être mises en correspondance avec l'une ou l'autre des mesures.

Étape 10 Cochez la case **Match Tag Numbers** (Correspondance des numéros de balise) pour redistribuer les routes dans la table de routage qui correspondent aux balises spécifiées. Si vous spécifiez plusieurs numéros de balise, les routes peuvent être mises en correspondance avec l'une ou l'autre des mesures.

Étape 11 Cliquez sur OK.

Étape 12 Cliquez sur Apply (appliquer).

Configurer les filtres de chemin AS

Un filtre de chemin AS vous permet de filtrer le message de mise à jour de routage à l'aide de listes d'accès et d'examiner les préfixes individuels dans un message de mise à jour. Si un préfixe dans le message de mise à jour correspond aux critères de filtre, ce préfixe individuel est filtré ou accepté selon l'action configurée pour l'entrée de filtre. Cette section décrit les étapes requises pour configurer les filtres de chemin AS.



Remarque Les listes d'accès du chemin AS ne sont pas les mêmes que les ACL normales du pare-feu.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **AS Path Filters (Filtres de chemin AS)**.

Étape 2 Cliquez sur Add (ajouter).

La boîte de dialogue Add Filter (Ajouter un filtre) apparaît. À partir de cette boîte de dialogue, vous pouvez ajouter un nom de filtre, son accès à la redistribution (c'est-à-dire autoriser ou refuser) et son expression régulière.

Étape 3 Dans le champ Name (Nom), attribuez un nom au chemin de filtre AS.

Étape 4 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 5 Spécifiez l'expression régulière. Cliquez sur **Build** (Générer) pour créer une expression régulière.

Étape 6 Cliquez sur **Test** (Tester) pour tester si une expression régulière correspond à une chaîne de votre choix.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les règles de communauté

Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. Vous pouvez utiliser les listes de communautés pour créer des groupes de communautés à utiliser dans une clause de correspondance d'une feuille de route. Tout comme une liste d'accès, une série de listes de communautés peut être créée. Les instructions sont vérifiées jusqu'à ce qu'une correspondance soit trouvée. Dès qu'une instruction est satisfaite, le test est terminé. Cette section décrit les étapes requises pour configurer les règles de communauté.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **Community Rules (Règles de communauté)** > **.**

Étape 2 Cliquez sur Add (ajouter).

La boîte de dialogue Add Community Rule (Ajouter une règle de communauté) apparaît. À partir de cette boîte de dialogue, vous pouvez ajouter un nom de règle, un type de règle, son accès de redistribution (c'est-à-dire autoriser ou refuser) et des communautés spécifiques.

Étape 3 Dans le champ Rule Name (Nom de la règle), saisissez un nom pour la règle de communauté.

Étape 4 Cliquez sur le bouton radio Standard ou Expanded (Étendu) pour indiquer le type de règle de communauté.

Étape 5 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 6 Pour ajouter des règles de communauté standard :

a) Dans le champ Communautés, spécifiez un numéro de communauté. Les valeurs valides sont comprises entre 1 et 4294967200.

b) (Facultatif) Cochez la case Internet (communauté connue) pour spécifier la communauté Internet. Les routages de cette communauté sont annoncés à tous les homologues (internes et externes).

c) (Facultatif) Cochez la case Do not advertise to any peers (Ne pas annoncer aux homologues) (communauté connue) pour spécifier la communauté sans annonce. Les routages de cette communauté ne sont annoncés à aucun homologue (interne ou externe).
d) (Facultatif) Cochez la case Do not export to next AS (Ne pas exporter vers le prochain AS) (communauté connue) pour spécifier la communauté sans exportation. Les routes avec cette communauté sont annoncées uniquement aux homologues dans le même système autonome ou uniquement aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.

Étape 7 Pour ajouter des règles de communauté étendues :

a) Dans le champ**Regular Expression** (Expression régulière), saisissez une expression régulière. Sinon, cliquez sur **Build** (Générer) pour créer une expression régulière.
b) Cliquez sur **Test** (Tester) pour examiner si l'expression régulière créée correspond à une chaîne de votre choix.

Étape 8 Cliquez sur OK.

Étape 9 Cliquez sur Apply (appliquer).

Configurer les paramètres de la famille d'adresses IPv4

Les paramètres IPv4 pour le BGP peuvent être configurés à partir de l'option de famille IPv4 dans la configuration du BGP. La section de la famille IPv4 comprend des sous-sections pour les paramètres généraux, les paramètres d'adresse d'agrégation, les paramètres de filtrage et les paramètres de voisin. Chacune de ces sous-sections vous permet de personnaliser les paramètres propres à la famille IPv4.

Configurer les paramètres généraux de la famille IPv4

Cette section décrit les étapes requises pour configurer les paramètres IPv4 généraux.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur General (Général).

Le volet de configuration générale des paramètres BGP de la famille IPv4 s'affiche.

Étape 3 Spécifiez les distances externe, interne et locale dans la zone Administration Distances (Distances administratives).

Étape 4 Dans la liste déroulante Learning Routes Map (Carte de routage apprise), choisissez un nom de carte de routage. Cliquez sur **Manage** (Gérer) pour ajouter et configurer des cartes de routage.

Étape 5 (Facultatif) Cochez la case **Generate Default Route** (Générer une route par défaut) pour configurer un processus de routage BGP afin de distribuer une route par défaut (réseau 0.0.0.0).

Étape 6 (Facultatif) Cochez la case **Summarize subnet routes into network-level routes** (Résumé des routes de sous-réseau en routes de niveau réseau) pour configurer la synthèse automatique des routes de sous-réseau en routes de niveau réseau.

Étape 7 (Facultatif) Cochez la case **Advertise inactive routes** (Annoncer les routes inactives) pour annoncer les routes qui ne sont pas installées dans la base d'informations de routage (RIB).

Étape 8 (Facultatif) Cochez la case **Redistribute iBGP into an IGP** (Redistribuer l'IBGP dans un IGP) pour configurer la redistribution iBGP dans un protocole de passerelle intérieure (IGP), comme IS-IS ou OSPF.

Étape 9 (Facultatif) Saisissez un intervalle d'analyse (en secondes) pour les routeurs BGP pour la validation du saut suivant dans le champ **Scanning Interval** (Intervalle d'analyse). Les valeurs valides sont comprises entre 5 et 60 secondes.

Étape 10 (Facultatif) Cochez la case **Enable address tracking** (Activer le suivi des adresses) pour activer le suivi des adresses du saut suivant du BGP. Spécifiez l'intervalle de délai entre les vérifications sur les routes de saut suivant mises à jour et installées dans la table de routage dans le champ **Delay Interval** (Intervalle de délai).

Étape 11 (Facultatif) Spécifiez le nombre maximal de routes iBGP (Protocole Border Gateway Protocol) parallèles internes qui peuvent être installées dans une table de routage dans le champ **Number of Paths** (Nombre de chemins), puis cochez la case **iBGP multipaths** (Chemins multiples iBGP).

Étape 12 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres d'adresse globale de la famille IPv4

Cette section décrit les étapes requises pour définir l'agrégation de routes spécifiques en une seule route.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Aggregate Address** (Adresse agrégée).

Le volet de configuration des paramètres d'adresse agrégée s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Aggregate Address (Ajouter une adresse agrégée) s'affiche.

Étape 4 Spécifiez un objet réseau dans le champ **Network** (Réseau).

Étape 5 Cochez la case **Generate autonomous system set path information** (Générer des renseignements sur le chemin d'accès au système autonome) pour générer des renseignements sur le chemin d'accès au système autonome.

Étape 6 Cochez la case **Filters all more-specific routes from the updates** (Filtrer toutes les routes plus spécifiques à partir des mises à jour) pour filtrer toutes les routes plus spécifiques à partir des mises à jour.

Étape 7 Choisissez une carte de routage dans la liste déroulante Attribute Map (Carte d'attribut). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une carte de routage.

Étape 8 Choisissez une carte de routage dans la liste déroulante Advertise Map (Carte d'annonce). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route.

Étape 9 Choisissez une carte de routage dans la liste déroulante Suppress Map (Carte de suppression). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route.

Étape 10 Cliquez sur **OK**.

Étape 11 Spécifiez une valeur pour la minuterie d'agrégation (en secondes) dans le champ **Aggregate Timer** (Minuterie d'agrégation). Les valeurs valides sont 0 ou toute valeur comprise entre 6 et 60.

Étape 12 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de filtrage de la famille IPv4

Cette section décrit les étapes requises pour filtrer les routes ou les réseaux reçus dans les mises à jour BGP entrantes.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Filtering** (Filtrage).

Le volet Define filters for BGP updates (Définir les filtres pour les mises à jour du BGP) s'affiche.

Étape 3 Cliquez sur **Add** (ajouter).

Le volet Add Filter (Ajouter un filtre) s'affiche.

Étape 4 Choisissez une direction dans la liste déroulante Direction. La direction spécifie si le filtre doit être appliqué aux mises à jour entrantes ou sortantes.

Étape 5 Choisissez une liste d'accès standard dans la lise déroulante Access List (Liste d'accès). Cliquez sur **Manage** (Gérer) pour ajouter une nouvelle ACL.

Étape 6 Pour les filtres sortants, vous pouvez éventuellement spécifier les types de routes distribués.

a) Choisissez une option dans la liste déroulante Protocol (Protocole).

Vous pouvez choisir un protocole de routage, par exemple, **BGP**, **EIGRP**, **OSPF** ou **RIP**.

Choisissez **Connected** (Connecté) pour filtrer les homologues et les réseaux appris par le biais des routes connectées.

Choisissez **Static** (Statique) pour filtrer les homologues et les réseaux appris par le biais des routes statiques.

b) Si vous avez choisi BGP, EIGRP ou OSPF, choisissez également le **Process ID** (ID de processus) pour ce protocole.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de voisin BGP de la famille IPv4

Cette section décrit les étapes requises pour définir les voisins BGP et les paramètres de voisins.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** >**Routing (Routage)** **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Neighbor** (Voisin).

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Cliquez sur **General** (Général) dans le volet de gauche.

Étape 5 Saisissez une adresse IP de voisin BGP dans le champ **IP Address** (Adresse IP). Cette adresse IP est ajoutée à la table des voisins BGP.

Étape 6 Saisissez le système autonome auquel le voisin BGP appartient dans le champ **Remote AS** (AS distant).

Étape 7 (Facultatif) Dans le champ **Description**, saisissez la description du voisin BGP.

Étape 8 (Facultatif) Cochez la case **Shutdown neighbor administratively** (Arrêter le voisin administrativement) pour désactiver un groupe de voisins ou d'homologues.

Étape 9 (Facultatif) Cochez la case **Enable address family** (Activer la famille d'adresses) pour activer la communication avec le voisin BGP.

Étape 10 (Facultatif) Cochez la case **Global Restart Functionality for this peer** (Fonctionnalité de redémarrage global pour cet homologue) pour activer ou désactiver la capacité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin ou un groupe d'homologues ASA.

Remarque Cette option est activée lorsque le périphérique est en mode haute disponibilité ou lorsqu'une grappe L2 (tous les nœuds du même réseau) est configurée.

Étape 11 (Facultatif) Pour mettre à jour une interface en tant que source pour le voisinage BGP, sélectionnez l'interface dans la liste déroulante **Update-Source** (Mettre à jour la source).

Remarque Si vous mettez à jour l'interface de boucle avec retour comme source pour le voisinage BGP, l'adresse IP de l'interface de boucle avec retour est annoncée sur le réseau. L'interface de boucle avec retour agit en tant qu'homologue eBGP et participe au routage. Comme l'interface de boucle avec retour est stable lorsqu'elle est activée et reste disponible jusqu'à ce qu'elle soit administrativement arrêtée, l'ASA est toujours accessible sur l'adresse IP de l'interface de boucle avec retour.

Étape 12 Cliquez sur **Filtering** (Filtrage) dans le volet de gauche.

Étape 13 (Facultatif) Choisissez la liste de contrôle d'accès entrant ou sortant appropriée dans la zone Filter routes using an access list (Filtrer les routes à l'aide d'une liste d'accès) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour ajouter une ACL et des ACE au besoin.

Étape 14 (Facultatif) Choisissez les cartes de routage entrantes ou sortantes appropriées dans la zone Filter routes using a route map (Filtrer les routes à l'aide d'une carte de routage) pour appliquer une carte de routage aux routes entrantes ou sortantes. Cliquez sur **Manage** (Gérer) pour configurer une carte de routage.

Étape 15 (Facultatif) Choisissez la liste de préfixes entrants ou sortants appropriée dans la zone Filter routes using a prefix list (Filtrer les routes à l'aide d'une liste de préfixes) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les listes de préfixes.

Étape 16 (Facultatif) Choisissez le filtre de chemin AS entrant ou sortant approprié dans la zone Filter routes using AS path filter (Filtrer les routes à l'aide d'un filtre de chemin AS) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les filtres de chemin AS.

Étape 17 (Facultatif) Cochez la case **Limit the number of prefixes allowed from the neighbor** (Limiter le nombre de préfixes autorisés du voisin) pour contrôler le nombre de préfixes qui peuvent être reçus d'un voisin.

- Saisissez le nombre maximum de préfixes autorisés pour un voisin spécifique dans le champ **Maximum prefixes** (Nombre maximum de préfixes).

- Dans le champ **Threshold level** (Niveau de seuil), saisissez le pourcentage (du maximum) à partir duquel le routeur commence à générer un message d'avertissement. Les valeurs valides sont des entiers compris entre 1 et 100. La valeur par défaut est 75.
- (Facultatif) Cochez la case **Control prefixes received from a peer** (Contrôle des préfixes reçus d'un homologue) pour spécifier des contrôles supplémentaires pour les préfixes reçus d'un homologue. Effectuez l'une des opérations suivantes :
  - Cliquez sur **Terminate peering when prefix limit is exceeded** (Mettre fin au jumelage lorsque la limite de préfixes est dépassée) pour arrêter le voisin BGP lorsque la limite de préfixe est atteinte. Précisez l'intervalle après lequel le voisin BGP redémarrera dans le champ Restart interval (intervalle de redémarrage).
  - Cliquez sur **Give only warning message when prefix limit is exceeded** (Envoyer uniquement un message d'avertissement lorsque la limite de préfixe est dépassée) pour générer un message de journal lorsque la limite de préfixe maximale est dépassée. Dans ce cas, le voisin BGP ne sera pas interrompu.

Étape 18 Cliquez sur **Routes** dans le volet de gauche.

Étape 19 Saisissez l'intervalle minimal (en secondes) entre l'envoi des mises à jour de routage de BGP dans le champ **Advertisement Interval** (intervalle des annonces).

Étape 20 (Facultatif) Cochez la case **Generate Default route** (Générer une route par défaut) pour permettre au routeur local d'envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut.

- Choisissez la carte de routage qui permet l'injection conditionnelle de la route 0.0.0.0 dans la liste déroulante Route map (Carte de routage). Cliquez sur **Manage** (Gérer) pour ajouter et configurer une carte de routage.

Étape 21 (Facultatif) Pour ajouter des routes annoncées sous condition, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) dans la section Conditionly Advertise Routes (Routes annoncées sous condition).
b) Choisissez la carte de routage qui sera annoncée dans la liste déroulante Advertise Map (Carte d'annonce) si les conditions de la carte existante ou inexistante sont remplies.
c) Effectuez l'une des opérations suivantes :
   - Cliquez sur **Exist Map** (Carte existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
   - Cliquez sur **Non-exist Map** (Carte non existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
d) Cliquez sur **Ok**.

Étape 22 (Facultatif) Cochez la case **Remove private autonomous system (AS) numbers from outbound routing updates** (Supprimer les numéros de systèmes autonomes (AS) privés des mises à jour de routage sortantes) pour empêcher les numéros de système autonomes privés d'être annoncés sur les routes sortantes.

Étape 23 Cliquez sur **Timers** (Minuteries) dans le volet de gauche.

Étape 24 (Facultatif) Cochez la case Set timers for the BGP peer (Définir les minuteries pour l'homologue BGP) pour définir la fréquence keepalive, le délai de rétention et le délai de rétention minimum.

- Saisissez la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive au voisin dans le champ **Keepalive frequency** (Fréquence keepalive). Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 60 secondes.
- Dans le champ **Hold time** (Délai de rétention), saisissez l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est 180secondes.
- (Facultatif) Dans le champ Min Hold time (Délai de rétention min.), saisissez l'intervalle minimum (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort.



Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 25 Cliquez sur Advanced (Avancé) dans le volet de gauche.

Étape 26 (Facultatif) Cochez la case Enable Authentication (activer l'authentification) pour activer l'authentification MD5 sur une connexion TCP entre deux homologues BGP.

- Choisissez un type de chiffrement dans la liste déroulante Encryption Type (Type de chiffrement).
- Saisissez un mot de passe dans le champ **Password** (Mot de passe). Saisissez à nouveau le mot de passe dans le champ **Confirm Password** (Confirmer le mot de passe).

  Le mot de passe est sensible à la casse et peut comporter jusqu'à 25 caractères lorsque la commande service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces. Vous ne pouvez pas spécifier de mot de passe au format nombre-espace-caractère quelconque. L'espace après le numéro peut faire échouer l'authentification.

Étape 27 (Facultatif) Cochez la case **Send Community Attribute to this neighbor** (Envoyer l'attribut de communauté à ce voisin).

Étape 28 (Facultatif) Cochez la case **Use ASA as next hop for neighbor** (Utiliser l'ASA comme prochain saut pour le voisin) pour configurer le routeur comme prochain saut pour un voisin ou un groupe d'homologues qui communique avec BGP.

Étape 29 Effectuez l'une des opérations suivantes :

- Cliquez sur **Allow connections with neighbor that is not directly connected** (Autoriser les connexions avec le voisin qui n'est pas directement connecté) pour accepter et tenter des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement.
  - (Facultatif) Saisissez la durée de vie dans le champ **TTL hops** (Sauts TTL). Les valeurs valides sont comprises entre 1 et 255.
  - (Facultatif) Cochez la case **Disable connection verification** (Désactiver la vérification de connexion) pour désactiver la vérification de connexion afin d'établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour.
- Cliquez sur **Limit number of TTL hops to neighbor** (Limiter le nombre de sauts TTL vers le voisin) pour vous permettre de sécuriser une session d'homologation BGP.

- Saisissez le nombre maximal de sauts qui séparent les homologues eBGP dans le champ **Sauts TTL**. Les valeurs valides sont comprises entre 1 et 254.

Étape 30 (Facultatif) Dans le champ **Weight** (Pondération), saisissez une pondération pour la connexion du voisin BGP.

Étape 31 Choisissez la version BGP que l'ASA acceptera dans la liste déroulante **BGP version** (Version BGP).



Remarque La version peut être définie sur 2 pour forcer le logiciel à utiliser uniquement la version 2 avec le voisin spécifié. La valeur par défaut est d'utiliser la version 4 et de négocier dynamiquement à la baisse jusqu'à la version 2 si nécessaire.

Étape 32 (Facultatif) Cochez la case **TCP Path MTU Discovery** (Découverte MTU du chemin TCP) pour activer une session de transport TCP pour une session BGP.

Étape 33 Choisissez le **TCP connection mode** (Mode de connexion TCP) dans la liste déroulante du mode de transport TCP.

Étape 34 Cliquez sur **Migration** dans le volet gauche.

Étape 35 (Facultatif) Cochez la case **Customize the AS number for routes received from the neighbor** (Personnaliser le numéro AS pour les routes reçues du voisin) pour personnaliser l'attribut AS_PATH pour les routes reçues d'un voisin eBGP.

- Saisissez le numéro du système autonome local dans le champ **Local AS Number** (Numéro AS local). Les valeurs valides sont comprises entre 1 et 65 535.
- (Facultatif) Cochez la case **Do not prepend local AS number for routes received from neighbor** (Ne pas ajouter au début le numéro AS local pour les routes reçues du voisin). Le numéro AS local ne sera pas ajouté au début des routes reçues de l'homologue eBGP.
- (Facultatif) Cochez la case **Replace real AS number with local AS number in routes received from neighbor** (Remplacer le numéro AS réel par le numéro AS local dans les routes reçues du voisin). Le numéro AS du processus de routage local n'est pas ajouté au début.
- (Facultatif) Cochez la case **Accept either real AS number or local AS number in routes received from neighbor** (Accepter le numéro AS réel ou le numéro AS local dans les routes reçues du voisin).

Étape 36 Cliquez sur **OK**.

Étape 37 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres réseau IPv4

Cette section décrit les étapes requises pour définir les réseaux à annoncer par le processus de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Networks** (Réseaux).

Le volet Define networks to be advertised by the BGP routing process configuration (Définir les réseaux à annoncer par la configuration du processus de routage BGP) s'affiche.

Étape 3 Cliquez sur **Add** (ajouter).

Le volet Add Network (ajouter un réseau) s'affiche.

Étape 4 Spécifiez le réseau que BGP annoncera dans le champ **Address** (Adresse).



Remarque Pour qu'un préfixe de réseau soit annoncé, une voie de routage vers le périphérique doit exister dans la table de routage.

Étape 5 (Facultatif) Choisissez un masque de réseau ou de sous-réseau dans la liste déroulante **Netmask** (Masque réseau).

Étape 6 Choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à annoncer dans la liste déroulante **Route Map**. Cliquez sur Manage (Gérer) pour configurer ou ajouter une carte de routage.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de redistribution IPv4

Cette section décrit les étapes nécessaires pour définir les conditions de redistribution des routes d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)** > **.**

Étape 2 Cliquez sur **Redistribution**.

Le volet Redistribution s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Redistribution (ajouter une redistribution) s'affiche.

Étape 4 Choisissez le protocole à partir duquel vous souhaitez redistribuer les routes dans le domaine BGP dans la liste déroulante **Source Protocol** (Protocole source).

Étape 5 Choisissez un ID de processus pour le protocole source dans la liste déroulante **Process ID** (ID de processus).

Étape 6 (Facultatif) Saisissez une mesure pour la route redistribuée dans le champ **Metric** (Mesure).

Étape 7 Choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à annoncer dans la liste déroulante **Route Map** (Carte de routage). Cliquez sur **Manage** (Gérer) pour configurer ou ajouter une carte de routage.

Étape 8 Cochez une ou plusieurs des cases **Internal** (Interne), **External** (Externe) et **NSSA External match** (Correspondance externe de NSSA) pour redistribuer les routes à partir d'un réseau OSPF.

Cette étape s'applique uniquement à la redistribution à partir des réseaux OSPF.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres d'injection de route IPv4

Cette section décrit les étapes nécessaires pour définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)** > **.**

Étape 2 Cliquez sur **Route Injection** (Injection de route).

Le volet Route Injection (Injection de routage) s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Conditionally injected route (Ajouter une route injectée sous condition) s'affiche.

Étape 4 Choisissez la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale depuis la liste déroulante **Inject Map** (Carte d'injection).

Étape 5 Choisissez la carte de routage contenant les préfixes que le locuteur BGP suivra depuis la liste déroulante **Exist Map** (Carte existante).

Étape 6 Cochez la case **Injected routes will inherit the attributes of the aggregate route** (Les routes injectées hériteront des attributs de la route agrégée) pour configurer la route injectée pour qu'elle hérite des attributs de la route agrégée.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de la famille d'adresses IPv6

Les paramètres IPv6 pour le BGP peuvent être configurés à partir de l'option de famille IPv6 dans la configuration du BGP. La section de la famille IPv6 comprend des sous-sections pour les paramètres généraux, les paramètres d'adresse d'agrégation et les paramètres de voisin. Chacune de ces sous-sections vous permet de personnaliser les paramètres propres à la famille IPv6.

Cette section décrit comment personnaliser les paramètres de famille IPv6 du BGP.

Configurer les paramètres généraux de la famille IPv6

Cette section décrit les étapes requises pour configurer les paramètres IPv6 généraux.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur **General** (Général).

Le volet de configuration générale des paramètres BGP de la famille IPv6 s'affiche.

Étape 3 Spécifiez les distances externe, interne et locale dans la zone **Administration Route Distances** (Distances de la route administrative).

Étape 4 (Facultatif) Cochez la case **Generate Default Route** (Générer une route par défaut) pour configurer un processus de routage BGP afin de distribuer une route par défaut (réseau 0.0.0.0).

Étape 5 (Facultatif) Cochez la case **Advertise inactive routes** (Annoncer les routes inactives) pour annoncer les routes qui ne sont pas installées dans la base d'informations de routage (RIB).

Étape 6 (Facultatif) Cochez la case **Redistribute iBGP into an IGP** (Redistribuer l'IBGP dans un IGP) pour configurer la redistribution iBGP dans un protocole de passerelle intérieure (IGP), comme IS-IS ou OSPF.

Étape 7 (Facultatif) Saisissez un intervalle d'analyse (en secondes) pour les routeurs BGP pour la validation du saut suivant dans le champ **Scanning Interval** (Intervalle d'analyse). Les valeurs valides sont comprises entre 5 et 60 secondes.

Étape 8 (Facultatif) Spécifiez le nombre maximum de routes de protocole de passerelle frontière qui peuvent être installées dans une table de routage dans le champ **Number of paths** (Nombre de chemins).

Étape 9 (Facultatif) Cochez la case **IBGP multipaths** (Chemins multiples IBGP) et spécifiez le nombre maximum de routes iBGP (Protocole Border Gateway Protocol) parallèles internes qui peuvent être installées dans une table de routage dans le champ **Number of paths** (Nombre de chemins).

Étape 10 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres d'adresse globale de la famille IPv6

Cette section décrit les étapes requises pour définir l'agrégation de routes spécifiques en une seule route.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur **Aggregate Address** (Adresse agrégée).

Le volet de configuration des paramètres d'adresse agrégée s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Aggregate Address (Ajouter une adresse agrégée) s'affiche.

Étape 4 Indiquez une adresse IPv6 dans le champ **IPv6/Address Mask** (IPv6/Masque d'adresse). Par ailleurs, parcourez la liste pour ajouter un objet réseau.

Étape 5 Cochez la case **Generate autonomous system set path information** (Générer des renseignements sur le chemin d'accès au système autonome) pour générer des renseignements sur le chemin d'accès au système autonome. Le chemin annoncé pour cette route sera un AS_SET composé de tous les éléments contenus dans tous les chemins résumés.

Remarque N'utilisez pas cette forme de commande aggregate-address lors de l'agrégation de nombreux chemins, car cette route doit être continuellement retirée et mise à jour en tant que renseignements sur l'accessibilité du chemin au système autonome pour les modifications de routes résumées.

Étape 6 Cochez la case **Filters all more-specific routes from the updates** (Filtrer toutes les routes plus spécifiques à partir des mises à jour) pour filtrer toutes les routes plus spécifiques à partir des mises à jour. Cela crée non seulement la route agrégée, mais supprime également les annonces de routes plus spécifiques à tous les voisins.

Étape 7 Choisissez une carte de routage dans la liste déroulante **Attribute Map** (Carte d'attribut). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une carte de routage. Cela permet de modifier les attributs de la route agrégée.

Étape 8 Choisissez une carte de routage dans la liste déroulante **Advertise Map** (Carte d'annonce). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route. Cela sélectionne des routes spécifiques qui seront utilisées pour créer différents composants de la route agrégée.

Étape 9 Choisissez une carte de routage dans la liste déroulante **Suppress Map** (Carte de suppression). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route. Cela crée la route agrégée, mais supprime l'annonce des routes spécifiées.

Étape 10 Cliquez sur **OK**.

Étape 11 Spécifiez une valeur pour la minuterie d'agrégation (en secondes) dans le champ **Aggregate Timer** (Minuterie d'agrégation). Les valeurs valides sont 0 ou toute valeur comprise entre 6 et 60. Cela spécifie l'intervalle auquel les routes seront agrégées. La valeur par défaut est de 30 secondes.

Étape 12 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de voisin BGP de la famille IPv6

Cette section décrit les étapes requises pour définir les voisins BGP et les paramètres de voisins.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)**

Étape 2 Cliquez sur **Neighbor** (Voisin).

Étape 3 Cliquez sur **Add** (Ajouter).

Étape 4 Cliquez sur **General** (Général) dans le volet de gauche.

Étape 5 Saisissez une adresse IPv6 de voisin BGP dans le champ **IPv6 Address** (Adresse IPv6). Cette adresse IPv6 est ajoutée à la table des voisins BGP.

Étape 6 Saisissez le système autonome auquel le voisin BGP appartient dans le champ **Remote AS** (AS distant).

Étape 7 (Facultatif) Dans le champ **Description**, saisissez la description du voisin BGP.

Étape 8 (Facultatif) Cochez la case **Shutdown neighbor administratively** (Arrêter le voisin administrativement) pour désactiver un groupe de voisins ou d'homologues.

Étape 9 (Facultatif) Cochez la case **Enable address family** (Activer la famille d'adresses) pour activer la communication avec le voisin BGP.

Étape 10 (Facultatif) Cochez la case **Global Restart Functionality for this peer** (Fonctionnalité de redémarrage global pour cet homologue) pour activer ou désactiver la capacité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin ou un groupe d'homologues ASA.



Remarque Cette option est activée lorsque le périphérique est en mode haute disponibilité ou lorsqu'une grappe L2 (tous les nœuds du même réseau) est configurée.

Étape 11 (Facultatif) Pour mettre à jour une interface en tant que source pour le voisinage BGP, sélectionnez l'interface dans la liste déroulante **Update-Source** (Mettre à jour la source).



Remarque Si vous mettez à jour l'interface de boucle avec retour comme source pour le voisinage BGP, l'adresse IP de l'interface de boucle avec retour est annoncée sur le réseau. L'interface de boucle avec retour agit en tant qu'homologue eBGP et participe au routage. Comme l'interface de boucle avec retour est stable lorsqu'elle est activée et reste disponible jusqu'à ce qu'elle soit administrativement arrêtée, l'ASA est toujours accessible sur l'adresse IP de l'interface de boucle avec retour.

Étape 12 Cliquez sur **Filtering** (Filtrage) dans le volet de gauche.

Étape 13 (Facultatif) Choisissez les cartes de routage entrantes ou sortantes appropriées dans la zone **Filter routes using a route map** (Filtrer les routes à l'aide d'une carte de routage) pour appliquer une carte de routage aux routes entrantes ou sortantes. Cliquez sur **Manage** (Gérer) pour configurer une carte de routage.

Étape 14 (Facultatif) Choisissez la liste de préfixes entrants ou sortants appropriée dans la zone **Filter routes using a prefix list** (Filtrer les routes à l'aide d'une liste de préfixes) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les listes de préfixes.

Étape 15 (Facultatif) Choisissez le filtre de chemin AS entrant ou sortant approprié dans la zone **Filter routes using AS path filter** (Filtrer les routes à l'aide d'un filtre de chemin AS) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les filtres de chemin AS.

Étape 16 (Facultatif) Cochez la case **Limit the number of prefixes allowed from the neighbor** (Limiter le nombre de préfixes autorisés du voisin) pour contrôler le nombre de préfixes qui peuvent être reçus d'un voisin.

Étape 17 Saisissez le nombre maximum de préfixes autorisés pour un voisin spécifique dans le champ **Maximum prefixes** (Nombre maximum de préfixes).

Étape 18 Dans le champ **Threshold level** (Niveau de seuil), saisissez le pourcentage (du maximum) à partir duquel le routeur commence à générer un message d'avertissement. Les valeurs valides sont des entiers compris entre 1 et 100. La valeur par défaut est 75.

Étape 19 (Facultatif) Cochez la case **Control prefixes received from a peer** (Contrôle des préfixes reçus d'un homologue) pour spécifier des contrôles supplémentaires pour les préfixes reçus d'un homologue. Effectuez l'une des opérations suivantes :

- Cliquez sur **Terminate peering when prefix limit is exceeded** (Mettre fin au jumelage lorsque la limite de préfixes est dépassée) pour arrêter le voisin BGP lorsque la limite de préfixe est atteinte. Précisez l'intervalle après lequel le voisin BGP redémarrera dans le champ **Restart interval** (intervalle de redémarrage).

- Cliquez sur **Give only warning message when prefix limit is exceeded** (Envoyer uniquement un message d'avertissement lorsque la limite de préfixe est dépassée) pour générer un message de journal lorsque la limite de préfixe maximale est dépassée. Dans ce cas, le voisin BGP ne sera pas interrompu.

Étape 20 Cliquez sur **Routes** dans le volet de gauche.

Étape 21 Saisissez l'intervalle minimum (en secondes) entre l'envoi des mises à jour de routage BGP dans le champ **Advertisement Interval** (Intervalle des annonces).

Étape 22 (Facultatif) Cochez la case **Generate Default route** (Générer une route par défaut) pour permettre au routeur local d'envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut.

Étape 23 Choisissez la carte de routage qui permet l'injection conditionnelle de la route 0.0.0.0 dans la liste déroulante **Route map** (Carte de routage). Cliquez sur **Manage** (Gérer) pour ajouter et configurer une carte de routage.

Étape 24 (Facultatif) Pour ajouter des routes annoncées sous condition, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) dans la section Conditionly Advertise Routes (Routes annoncées sous condition).

b) Choisissez la carte de routage qui sera annoncée dans la liste déroulante **Advertise Map** (Carte d'annonce) si les conditions de la carte existante ou inexistante sont remplies.

c) Effectuez l'une des opérations suivantes :

- Cliquez sur **Exist Map** (Carte existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- Cliquez sur **Non-exist Map** (Carte non existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.

d) Cliquez sur **Ok**.

Étape 25 (Facultatif) Cochez la case **Remove private autonomous system (AS) numbers from outbound routing updates** (Supprimer les numéros de systèmes autonomes (AS) privés des mises à jour de routage sortantes) pour empêcher les numéros de système autonomes privés d'être annoncés sur les routes sortantes.

Étape 26 Cliquez sur **Timers** (Minuteries) dans le volet de gauche.

Étape 27 (Facultatif) Cochez la case **Set timers for the BGP peer** (Définir les minuteries pour l'homologue BGP) pour définir la fréquence keepalive, le délai de rétention et le délai de rétention minimum.

Étape 28 Saisissez la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive au voisin dans le champ **Keepalive frequency** (Fréquence keepalive). Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 60 secondes.

Étape 29 Dans le champ **Hold time** (Délai de rétention), saisissez l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est 180secondes.

Étape 30 (Facultatif) Dans le champ **Min Hold time** (Délai de rétention min.), saisissez l'intervalle minimum (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort.

Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 31 Cliquez sur **Advanced** (Avancé) dans le volet de gauche.

Étape 32 (Facultatif) Cochez la case **Enable Authentication** (Activer l'authentification) pour activer l'authentification MD5 sur une connexion TCP entre deux homologues BGP.

Étape 33 Choisissez un type de chiffrement dans la liste déroulante **Encryption Type** (Type de chiffrement).

Étape 34 Saisissez un mot de passe dans le champ **Password** (Mot de passe). Saisissez votre nouveau mot de passe dans le champ **Confirm Password** (Confirmer le mot de passe).

Le mot de passe est sensible à la casse et peut comporter jusqu'à 25 caractères lorsque la commande service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces. Vous ne pouvez pas spécifier de mot de passe au format nombre-espace-caractère quelconque. L'espace après le numéro peut faire échouer l'authentification.

Étape 35 (Facultatif) Cochez la case **Send Community Attribute to this neighbor** (Envoyer l'attribut de communauté à ce voisin).

Étape 36 (Facultatif) Cochez la case **Use ASA as next hop for neighbor** (Utiliser l'ASA comme prochain saut pour le voisin) pour configurer le routeur comme prochain saut pour un voisin ou un groupe d'homologues qui communique avec BGP.

Étape 37 Effectuez l'une des opérations suivantes :

- Cliquez sur **Allow connections with neighbor that is not directly connected** (Autoriser les connexions avec le voisin qui n'est pas directement connecté) pour accepter et tenter des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement.
  - (Facultatif) Saisissez la durée de vie dans le champ **TTL hops** (Sauts TTL). Les valeurs valides sont comprises entre 1 et 255.
  - (Facultatif) Cochez la case **Disable connection verification** (Désactiver la vérification de connexion) pour désactiver la vérification de connexion afin d'établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour.
- Cliquez sur **Limit number of TTL hops to neighbor** (Limiter le nombre de sauts TTL vers le voisin) pour vous permettre de sécuriser une session d'homologation BGP. Saisissez le nombre maximal de sauts qui séparent les homologues eBGP dans le champ Sauts TTL. Les valeurs valides sont comprises entre 1 et 254.

Étape 38 (Facultatif) Dans le champ **Weight** (Pondération), saisissez une pondération pour la connexion du voisin BGP.

Étape 39 Choisissez la version BGP que l'ASA acceptera dans la liste déroulante BGP version (Version BGP).

Remarque La version peut être définie sur 2 pour forcer le logiciel à utiliser uniquement la version 2 avec le voisin spécifié. La valeur par défaut est d'utiliser la version 4 et de négocier dynamiquement à la baisse jusqu'à la version 2 si nécessaire.

Étape 40 (Facultatif) Cochez la case **TCP Path MTU Discovery** (Découverte MTU du chemin TCP) pour activer une session de transport TCP pour une session BGP.

Étape 41 Choisissez le **TCP connection mode** (Mode de connexion TCP) dans la liste déroulante du mode de transport TCP.

Étape 42 Cliquez sur **Migration** dans le volet gauche.

Étape 43 (Facultatif) Cochez la case **Customize the AS number for routes received from the neighbor** (Personnaliser le numéro AS pour les routes reçues du voisin) pour personnaliser l'attribut AS_PATH pour les routes reçues d'un voisin eBGP.

- Saisissez le numéro du système autonome local dans le champ Local AS Number (Numéro AS local). Les valeurs valides sont comprises entre 1 et 65 535.
- (Facultatif) Cochez la case Do not prepend local AS number for routes received from neighbor (Ne pas ajouter au début le numéro AS local pour les routes reçues du voisin). Le numéro AS local ne sera pas ajouté au début des routes reçues de l'homologue eBGP.
- (Facultatif) Cochez la case Replace real AS number with local AS number in routes received from neighbor (Remplacer le numéro AS réel par le numéro AS local dans les routes reçues du voisin). Le numéro AS du processus de routage local n'est pas ajouté au début.
- (Facultatif) Cochez la case Accept either real AS number or local AS number in routes received from neighbor (Accepter le numéro AS réel ou le numéro AS local dans les routes reçues du voisin).

Étape 44 Cliquez sur **OK**.

Étape 45 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres réseau IPv6

Cette section décrit les étapes requises pour définir les réseaux à annoncer par le processus de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur **Networks** (Réseaux).

Le volet Define the networks to be advertised by the BGP routing process configuration (Définir les réseaux à annoncer par la configuration du processus de routage BGP) s'affiche.

Étape 3 Cliquez sur **Add** (ajouter).

Le volet Add Network (ajouter un réseau) s'affiche.

Étape 4 (Facultatif) Dans le champ Prefix Name (nom du préfixe), précisez le nom de préfixe du client de délégation de préfixe DHCPv6 (voir Activer le client de délégation de préfixe IPv6).

Étape 5 Dans le champ**IPv6 Address/mask (adresse/masque IPv6**), précisez le réseau que BGP annoncera.

Si vous spécifiez le **nom de préfixe**, saisissez le préfixe et le masque de sous-réseau; le réseau annoncé se compose du préfixe délégué + du préfixe de sous-réseau.

Étape 6 Choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à annoncer dans la liste déroulante **Route Map**. Cliquez éventuellement sur **Manage** (Gérer) pour configurer ou ajouter une carte de routage.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de redistribution IPv6

Cette section décrit les étapes nécessaires pour définir les conditions de redistribution des routes d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur Redistribution.

Étape 3 Cliquez sur Add (ajouter).

Le volet Add Redistribution (ajouter une redistribution) s'affiche.

Étape 4 Dans la iste déroulante Source Protocol (Protocole source), choisissez le protocole à partir duquel vous souhaitez redistribuer les routes dans le domaine BGP.

Étape 5 Dans la liste déroulante Process ID (ID de processus), choisissez un ID de processus pour le protocole source. Cette option est disponible uniquement pour le protocole source OSPF.

Étape 6 (Facultatif) Dans le champ Metric (Mesure), saisissez une mesure pour la route redistribuée.

Étape 7 Dans la liste déroulante Route Map (Carte de routage), choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à redistribuer. Cliquez sur Manage (Gérer) pour configurer ou ajouter une carte de routage.

Étape 8 Cochez une ou plusieurs des cases Match (Correspondance) (interne, externe 1, externe 2, NSSA externe 1 et NSSA externe 2) pour redistribuer les routes à partir d'un réseau OSPF.

Cette étape s'applique uniquement à la redistribution à partir des réseaux OSPF.

Étape 9 Cliquez sur OK.

Étape 10 Cliquez sur Apply (appliquer).

Configurer les paramètres d'injection de route IPv6

Cette section décrit les étapes nécessaires pour définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Route Injection** (Injection de route).

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Conditionally injected route (Ajouter une route injectée sous condition) s'affiche.

Étape 4 Dans la liste déroulante **Inject Map** (Carte d'injection), choisissez la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale.

Étape 5 Dans la liste déroulante**Exist Map** (Carte existante), choisissez la carte de routage contenant les préfixes que le locuteur BGP suivra.

Étape 6 Cochez la case **Injected routes will inherit the attributes of the aggregate route** (Les routes injectées hériteront des attributs de la route agrégée) pour configurer la route injectée pour qu'elle hérite des attributs de la route agrégée.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Supervision BGP

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage BGP. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande. En outre, vous pouvez désactiver la journalisation des messages de modification de voisin et des messages d'avertissement de voisin.

Pour superviser diverses statistiques de routage BGP, saisissez l'une des commandes suivantes :

Remarque Pour désactiver les messages du journal BGP, saisissez la commande **no bgp log-neighbor-changes** dans le mode de configuration du routeur. Cela désactive la journalisation des messages de modification de voisin. Saisissez cette commande en mode de configuration du routeur pour le processus de routage BGP. Par défaut, les modifications de voisins sont journalisées.

- **Monitoring (Supervision) > Routing (Routage) > BGP Neighbors (Voisins BGP)**

  Chaque ligne représente un voisin BGP. Pour chaque voisin, la liste comprend l'adresse IP, le numéro d'AS, l'ID de routeur, l'état (actif, inactif, etc.), la disponibilité, la capacité de redémarrage progressif, l'heure de redémarrage et l'heure du chemin obsolète.

- **Monitoring (Supervision) > Routing (Routage) > BGP Routes (Routes BGP)**

  Chaque ligne représente une route BGP. Pour chaque route, la liste comprend le code d'état, l'adresse IP, l'adresse du saut suivant, la mesure de la route, les valeurs de préférence locales, la pondération et le chemin.

Historique de BGP

Tableau 1 : Historique des fonctionnalités de BGP

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP	9.2(1)	Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole de passerelle frontière. Nous avons introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP Monitoring (Supervision BGP) > Routing (Routage) > BGP Neighbors (Voisins BGP), Monitoring (Supervision) > Routing (Routage) > BGP Routes (Routes BGP) Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Static Routes (Routes statiques) > Add (Ajouter) > Add Static Route (Ajouter une route statique) Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add (Ajouter) > Add Route Map (Ajouter une carte de routage)
Prise en charge BGP pour la mise en grappe d'ASA	9.3(1)	Nous avons ajouté la prise en charge de la mise en grappe de niveau 2 et de niveau 3. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv4 Family (Famille IPv4) > General (Général)
Prise en charge BGP pour la transmission sans interruption	9.3(1)	Nous avons ajouté la prise en charge de la transmission sans interruption. Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > General (Général), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv4 Family (Famille IPv4) > Neighbor (Voisin), Monitoring (Supervision) > Routing (Routage) > BGP Neighbors (Voisins BGP)
Prise en charge BGP pour les cartes annoncées	9.3(1)	Nous avons ajouté la prise en charge des cartes annoncées BGPv4. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv4 Family (Famille IPv4) > Neighbor (Voisin) > Add BGP Neighbor (Ajouter un voisin BGP) > Routes

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP pour IPv6	9.3(2)	Nous avons ajouté la prise en charge d'IPv6. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv6 Family (Famille IPv6)
Annonce de réseau IPv6 pour les préfixes délégués	9.6(2)	L'ASA prend désormais en charge le client de délégation de préfixe DHCPv6. L'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. Vous pouvez configurer le routeur BGP pour annoncer ces préfixes. Nous avons modifié l'écran suivant : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)** > **Networks (Réseaux)**
Prise en charge de l'interface de boucle avec retour pour le trafic BGP	9.18(2)	Vous pouvez utiliser une interface de boucle avec retour pour le trafic BGP. Commandes nouvelles/modifiées : **interface loopback**, **neighbor update-source** Écrans Nouveaux ou modifiés : • **Configuration (configuration)** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Loopback Interface (Ajouter une interface de boucle avec retour)**. • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family/IPv6 Family (Famille IPv4/famille IPv6)** > **Neighbor (Voisin)** > **Add (Ajouter)** > **General (Général)** La prise en charge d'ASDM a été ajoutée dans la version 7.19.
Prise en charge du redémarrage progressif pour IPv6	9.19(1)	Nous avons ajouté la prise en charge du redémarrage progressif pour la famille d'adresses IPv6.

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.