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).

À propos de BGP

BGP est un protocole de routage de systèmes inter et intra autonomes. Un système autonome est un réseau ou un groupe de réseaux soumis à une administration et à des politiques de routage communes. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP).

Quand utiliser 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 voisins BGP échangent des informations de routage complètes lors de la connexion TCP entre voisins est établie pour la première fois. Lorsque des modifications de la table de routage sont détectées, les routeurs BGP envoient à leurs voisins uniquement les routes qui ont été modifiées. Les routeurs BGP n'envoient pas de mises à jour de routage périodiques et les mises à jour de routage BGP n'annoncent que le chemin optimale vers un réseau de destination.

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.

Les routes apprises via BGP ont des propriétés utilisées pour déterminer la meilleure route vers une destination, lorsque plusieurs chemins existent vers une destination particulière. Ces propriétés sont appelées attributs BGP et sont utilisées dans le processus de sélection 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 pondération, l'attribut de préférence locale se propage dans tout le système autonome local. S'il y a plusieurs points de sortie du système autonome, le point de sortie avec l'attribut de préférence locale le plus élevé est utilisé comme point de sortie pour une route 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.

Sélection du chemin BGP

BGP peut recevoir plusieurs annonces pour la même route provenant de différentes sources. BGP sélectionne un seul chemin comme meilleur chemin. Lorsque ce chemin est sélectionné, BGP le met dans la table de routage IP et propage le chemin à ses voisins. BGP utilise les critères suivants, dans l'ordre présenté, pour sélectionner un chemin pour une destination :

- Si le chemin précise un saut suivant inaccessible, supprimez la mise à jour.
- Privilégiez le chemin avec la pondération la plus élevée.
- 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.
- 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).
- 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.
- 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.
- Si les deux chemins sont externes, privilégiez le chemin qui a été reçu en premier (le plus ancien).
- 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.

- Privilégiez le chemin qui provient de l’adresse du voisin le plus bas.

Chemins multiples BGP

Les chemins BGP multiples permettent l’installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination. Le trafic vers le préfixe de destination est ensuite partagé sur tous les chemins installés.

Ces chemins sont installés dans le tableau avec le meilleur chemin pour le partage de la charge. Les chemins multiples de 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 avoir ces caractéristiques égales aux caractéristiques du 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 de BGP)

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

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

BGP insère jusqu’à *n* derniers chemins reçus de candidats aux chemins multiples dans la table de routage IP, *n* étant le nombre de routes à installer dans la table de routage, comme spécifié lorsque vous configurez BGP multi-chemins. 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 Le prochain-saut-self équivalent est effectué sur le meilleur chemin sélectionné parmi les chemins multiples eBGP avant qu’il ne soit transmis aux homologues internes.

Lignes directrices BGP

Directives relatives au mode contextuel

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

Directives 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.

Directives IPv6

Prend en charge IPv6.

Directives 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.

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 7.

Étape 3 Configurer les listes de politiques, à la page 8.

Étape 4 Configurer les filtres de chemin AS, à la page 9.

Étape 5 Configurer les règles de communauté, à la page 10.

Étape 6 Configurer les paramètres de la famille d'adresses IPv4, à la page 11.

Étape 7 Configurer les paramètres de la famille d'adresses IPv6, à la page 25.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Les valeurs valides pour autonomous-num vont de 1 à 4294967295 et de 1.0 à XX.YY.

Étape 2 Ignorez les routes ayant des segments de chemin AS qui dépassent une valeur spécifiée :

bgp maxas-limit number

Exemple :

```
ciscoasa(config-router)# bgp maxas-limit 15
```

L'argument de nombre spécifie le nombre maximum de segments de système autonomes autorisés. Les valeurs valides sont comprises entre 1 et 254.

Étape 3 Journalisez les réinitialisations du voisin BGP :

changements journalisation voisin bgp

Étape 4 Activez BGP pour détecter automatiquement la meilleure MTU de chemin TCP pour chaque session BGP :

bgp transport path-mtu-discovery

Étape 5 Activez BGP pour mettre fin aux sessions BGP externes de tout homologue directement adjacent si le lien utilisé pour atteindre l'homologue tombe en panne; sans attendre l'expiration du délai d'attente :

bgp fast-external-fallover

Étape 6 Autorisez un processus de routage BGP à ignorer les mises à jour reçues d'un homologue BGP (eBGP) externe qui n'indique pas son numéro de système autonome (AS) comme premier segment de chemin AS dans l'attribut AS_PATH de la route entrante :

bgp enforce-first-as

Étape 7 Modifiez le format de correspondance d'affichage par défaut et d'expression régulière des numéros du système autonome BGP de 4 octets de texte (valeurs décimales) à la notation des points :

bgp asnotation dot

Étape 8 Ajustez les minuteries de réseau BGP :

timers bgp keepalive holdtime [min-holdtime]

Exemple :

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive : la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive à son homologue. La valeur par défaut est de 60 secondes.
- holdtime : 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 de 180 secondes.
- (Facultatif) min-holdtime : l'intervalle minimal (en secondes) après l'absence de réception de message keepalive d'un voisin indiquant que l'ASA déclare un voisin mort.

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

Étape 9 Activez la capacité de redémarrage progressif de BGP :

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

Exemple :

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time : période maximale (en secondes) pendant laquelle l'ASA attendra qu'un voisin compatible avec le redémarrage progressif reprenne son fonctionnement normal après un événement de redémarrage. La valeur par défaut est de 120 secondes. Les valeurs valides vont de 1 à 3 600 secondes.
- slatepath-time : période maximale (en secondes) pendant laquelle l'ASA conservera les chemins obsolètes pour un homologue en redémarrage. Tous les chemins obsolètes sont supprimés après l'expiration de cette minuterie. La valeur par défaut est 360 secondes. Les valeurs valides vont de 1 à 3 600 secondes.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Modifiez la valeur de préférence locale par défaut :

bgp default local-preference number

Exemple :

```
ciscoasa(config-router)# bgp default local-preference 500
```

L'argument number est toute valeur comprise entre 0 et 4294967295. Des valeurs plus élevées indiquent une préférence plus élevée.

La valeur par défaut est 100.

Étape 3 Activez la comparaison du Discriminateur multi-sortie (MED) entre les chemins appris des voisins dans différents systèmes autonomes :

bgp always-compare-med

Étape 4 Comparez les routes similaires reçues des homologues BGP externes (eBGP) pendant le processus de sélection du meilleur chemin et faites passer le meilleur chemin à la route ayant le plus petit ID de routeur :

bgp bestpath compare-routerid

Étape 5 Sélectionnez le meilleur chemin MED annoncé à partir de l'AS voisin :

bgp deterministic-med

Étape 6 Définissez un chemin avec un attribut MED manquant comme chemin le moins préféré :

bgp bestpath med missing-as-worst

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 Créez une liste de politiques BGP.

policy-list *policy_list_name* {**permit** | **deny**}

Le mot clé **permit** autorise l'accès pour les conditions de correspondance.

Le mot clé **deny** refuse l'accès pour les conditions de correspondance.

Exemple :

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

Étape 2 Distribuez les routes dont le prochain saut se trouve hors de l'une des interfaces spécifiées :

match interface [*interface_name* [*interface_name*] […]]

Exemple :

```
ciscoasa(config-policy-list)# match interface outside
```

Étape 3 Redistribuez les routes en faisant correspondre l'un ou l'ensemble des éléments suivants : l'adresse de destination, l'adresse du routeur du saut suivant et la source du routeur/serveur d'accès :

match ip {**address** | **next-hop** | **route-source**}

Étape 4 Faites correspondre un chemin d'accès au système autonome BGP :

match as-path

Étape 5 Faites correspondre une communauté BGP :

match community {*community-list_name* | **exact-match**}

- *community-list_name* : une ou plusieurs listes de communautés.
- **exact-match** : indique qu'une correspondance exacte est requise. Toutes les communautés et seulement les communautés spécifiées doivent être présentes.

Exemple :

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

Étape 6 Redistribuez les routes avec les mesures spécifiées :

match metric *metric* [*metric* […]]

Étape 7 Redistribuez les routes dans la table de routage qui correspondent aux balises spécifiées :

match tag *tag* [*tag* […]]

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

Configurez un filtre de chemin de système autonome à l'aide d'une expression régulière dans le mode de configuration globale :

as-path access-list acl-number {permit|deny} regexp

Exemple :

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number* : numéro de liste d'accès du chemin AS. Cette valeur peut être comprise entre 1 et 500.
- regexp : expression régulière qui définit le filtre de chemin AS. Le numéro de système autonome est compris entre 1 et 65 535.

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

Créez ou configurez une liste de communautés BGP et contrôlez l'accès à celle-ci :

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

Exemple :

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise no-export
```

- standard : configure une liste de communautés standard en utilisant un nombre allant de 1 à 99 pour identifier un ou plusieurs groupes de communautés autorisés ou refusés.

- (Facultatif) community-number : communauté sous forme de numéro de 32 bits allant de 1 à 4294967200. Une seule communauté peut être saisie ou plusieurs communautés peuvent être saisies, chacune séparée par un espace.
- AA:NN : un numéro de système autonome et un numéro de réseau saisis dans le nouveau format de communauté de 4 octets. Cette valeur est configurée avec deux nombres de 2 octets séparés par deux points. Un nombre de 1 à 65 535 peut être entré pour chaque numéro de 2 octets. Une seule communauté peut être saisie ou plusieurs communautés peuvent être saisies, chacune séparée par un espace.
- (Facultatif) internet : spécifie la communauté Internet. Les routages de cette communauté sont annoncés à tous les homologues (internes et externes).
- (Facultatif) no-advertise : spécifie la communauté sans publicité. Les routages de cette communauté ne sont annoncés à aucun homologue (interne ou externe).
- (Facultatif) no-export : spécifie 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.
- (Facultatif) expanded : configure un numéro de liste de communautés étendu de 100 à 500 pour identifier un ou plusieurs groupes de communautés autorisés ou refusés.
- regexp : expression régulière qui définit le filtre de chemin AS. Le numéro de système autonome est compris entre 1 et 65 535.

  Remarque
  Les expressions régulières ne peuvent être utilisées qu'avec les listes de communautés étendues.

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 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 (Facultatif) Configurez un ID de routeur fixe pour le processus de routage BGP local :

bgp router-id A.B.C.D

Exemple :

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

L'argument A.B.C.D spécifie un identifiant de routeur sous la forme d'une adresse IP. Si vous ne spécifiez pas d'ID de routeur, il est automatiquement attribué.

Étape 4 (Facultatif) Configurez un ensemble d'adresses IP en grappe en mode d'interface individuelle (L3) :

bgp router-id cluster-pool

Exemple :

```
ciscoasa(config-router-af)# bgp router-id cp
```

Remarque
Dans une grappe L3, vous ne pouvez pas définir un voisin BGP comme l'une des adresses IP de l'ensemble de grappe.

Étape 5 Configurez la distance administrative des routes BGP :

distance bgp external-distance internal-distance local-distance

Exemple :

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance : distance administrative pour les routes BGP externes. Les routes sont externes lorsqu'elles sont apprises à partir d'un système autonome externe. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- internal-distance : distance administrative pour les routes BGP internes. Les routes sont internes lorsqu'elles sont apprises de l'homologue dans le système autonome local. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- local-distance : distance administrative pour les routes BGP locales. Les routes locales sont les réseaux répertoriés avec une commande de configuration de routeur de réseau, souvent comme portes dérobées, pour le routeur ou pour les réseaux qui sont redistribués à partir d'un autre processus. La plage de valeurs pour cet arguments est comprise entre 1 et 255.

Étape 6 Modifiez les valeurs des mesures et des balises lorsque le tableau de routage IP est mis à jour avec les routes apprises du protocole BGP :

table-map {WORD|route-map_name}

Exemple :

```
ciscoasa(config-router-af)# table-map example1
```

L'argument route-map_name spécifie le nom de la carte de routage de la commande route-map.

Étape 7 Configurez un processus de routage BGP pour distribuer une route par défaut (réseau 0.0.0.0) :

default-information originate

Étape 8 Configurez la synthèse automatique des routes de sous-réseau dans les routes au niveau du réseau :

auto-summary

Étape 9 Supprimez l'annonce des routes qui ne sont pas installées dans la base d'informations de routage (RIB) :

bgp suppress-inactive

Étape 10 Synchronisez le BGP avec votre système IGP (protocole de passerelle intérieure) :

synchronisation

Étape 11 Configurez la redistribution iBGP dans un IGP, tel que OSPF :

bgp redistribute-internal

Étape 12 Configurez des intervalles d'analyse des routeurs BGP pour la validation du saut suivant :

bgp scan-time scanner-interval

Exemple :

```
ciscoasa(config-router-af)# bgp scan-time 15
```

L'argument scanner-interval spécifie l'intervalle d'analyse des renseignements de routage BGP. Les valeurs valides sont comprises entre 5 et 60 secondes. La valeur par défaut est de 60 secondes.

Étape 13 Configurez le suivi des adresses du saut suivant du protocole BGP :

bgp nexthop trigger {delay seconds|enable}

Exemple :

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger : spécifie l'utilisation du suivi d'adresses du saut suivant du protocole BGP. Utilisez ce mot clé avec le mot clé delay pour modifier le délai de suivi du saut suivant. Utilisez ce mot clé avec le mot clé enable pour activer le suivi d'adresses du saut suivant.
- delay : modifie l'intervalle de délai entre les vérifications sur les routes de saut suivant mises à jour installées dans la table de routage.
- seconds : spécifie le délai en secondes. La plage se situe entre 0 et 100. La valeur par défaut est 5.
- enable : active immédiatement le suivi des adresses du saut suivant du protocole BGP.

Étape 14 Contrôlez le nombre maximum de routes iBGP parallèles qui peuvent être installées dans une table de routage :

maximum-paths {number_of_paths|ibgp number_of_paths}

Exemple :

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Remarque
Si le mot clé ibgp n'est pas utilisé, l'argument number_of_paths contrôle le nombre maximum de routes EBGP parallèles.

L'argument number_of_paths spécifie le nombre de routes à installer dans la table de routage. Les valeurs valides sont comprises entre 1 et 8.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Créez une entrée agrégée dans une base de données BGP :

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

Exemple :

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address : l'adresse agrégée.
- mask : le masque agrégé.
- map-name : la carte de routage.
- (Facultatif) as-set : génère des renseignements sur le chemin de définition du système autonome.

- (Facultatif) summary-only : filtre toutes les routes plus spécifiques à partir des mises à jour.
- (Facultatif) Suppress-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes à supprimer.
- (Facultatif) Advertise-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes afin de créer les communautés d'origine AS_SET.
- (Facultatif) Attribute-map map-name : spécifie le nom de la carte de routage utilisée pour définir l'attribut de la route agrégée.

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 Activez un processus de routage BGP et passez en mode de configuration du routeur :

router bgp *autonomous-num*

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [**unicast**]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Filtrez les routes ou les réseaux reçus dans les mises à jour BGP entrantes ou annoncés dans les mises à jour BGP sortantes :

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

L'argument *acl-number* spécifie le numéro de la liste d'accès IP. La liste d'accès définit les réseaux à recevoir et ceux à supprimer dans les mises à jour de routage.

Le mot clé **in** spécifie que le filtre doit être appliqué aux mises à jour BGP entrantes et **out** spécifie que le filtre doit être appliqué aux mises à jour BGP sortantes.

Pour les filtres sortants, vous pouvez éventuellement spécifier un protocole (**bgp**, **eigrp**, **ospf** ou **rip**) avec un numéro de processus (à l'exception du protocole RIP) à appliquer à la liste de distribution. Vous pouvez également filtrer selon que les homologues et les réseaux ont été appris par les routes **connected** ou **static**.

Exemple :

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

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 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Ajoutez une entrée au tableau de voisins BGP :

neighbor ip-address remote-as autonomous-number

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

Étape 4 (Facultatif) Désactivez un groupe de voisins ou d'homologues :

neighbor ip-address shutdown

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

Étape 5 Échangez des renseignements avec un voisin BGP :

neighbor ip-address activate

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

Étape 6 Activez ou désactivez la fonctionnalité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin BGP :

neighbor ip-address ha-mode graceful-restart [disable]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

(Facultatif) Le mot clé disable désactive la fonctionnalité de redémarrage progressif du BGP pour un voisin.

Étape 7 Distribuez les renseignements sur le voisin BGP comme spécifiés dans une liste d'accès :

neighbor {ip-address} distribute-list {access-list-name}{in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number : le numéro d'une liste d'accès standard ou étendue. La plage d'un numéro de liste d'accès standard va de 1 à 99. La plage d'un numéro de liste d'accès étendue va de 100 à 199.
- expanded-list-number : le numéro d'une liste d'accès étendue. La plage d'une liste d'accès étendue va de 1 300 à 2 699.
- access-list-name : le nom d'une liste d'accès standard ou étendue.
- prefix-list-name : le nom d'une liste de préfixes BGP.
- in : la liste d'accès est appliquée aux annonces entrantes de ce voisin.
- out : signifie que la liste d'accès est appliquée aux annonces sortantes vers ce voisin.

Étape 8 Appliquez une carte de routage aux routes entrantes ou sortantes :

neighbor {ip-address} route-map map-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

Le mot clé dans applique une carte de routage aux routes entrantes.

Le mot clé out applique une carte de routage aux routes sortantes.

Étape 9 Distribuez les renseignements sur le voisin BGP comme spécifiés dans une liste de préfixes :

neighbor {ip-address} prefix-list prefix-list-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

Le mot clé in implique que la liste de préfixes soit appliquée aux annonces entrantes de ce voisin.

Le mot clé out implique que la liste de préfixes soit appliquée aux annonces sortantes de ce voisin.

Étape 10 Configurez une liste de filtres :

neighbor {ip-address} filter-list access-list-number {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name : spécifie le numéro d'une liste d'accès de chemin au système autonome. Vous définissez cette liste d'accès avec la commande ip as-path access-list.
- in : signifie que la liste d'accès est appliquée aux annonces entrantes de ce voisin.
- out : signifie que la liste d'accès est appliquée aux annonces sortantes vers ce voisin.

Étape 11 Contrôlez le nombre de préfixes pouvant être reçus d'un voisin.

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum : le nombre maximum de préfixes autorisés pour ce voisin.
- (Facultatif) threshold : entier indiquant à quel pourcentage du maximum le routeur commence à générer un message d'avertissement. La plage se situe entre 1 et 100; la valeur par défaut est de 75 (pour cent).
- (Facultatif) restart interval : valeur entière (en minutes) qui spécifie l'intervalle de temps après lequel le voisin BGP redémarre.
- (Facultatif) warning-only : permet au routeur de générer un message de journal lorsque le nombre maximum de préfixes est dépassé, au lieu de mettre fin à l'homologation.

Étape 12 Autorisez un haut-parleur BGP (le routeur local) à envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut :

neighbor {ip-address} default-originate [route-map map-name]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

L'argument map-name est le nom de la carte de routage. La carte de routage permet l'injection conditionnelle de la route 0.0.0.0.

Étape 13 Définissez l'intervalle minimum entre l'envoi des mises à jour de routage BGP :

neighbor {ip-address} advertisement-interval seconds

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

L'argument seconds est le temps (en secondes). Les valeurs valides sont comprises entre 0 et 600.

Étape 14 Annoncez les routes dans le tableau BGP qui correspondent à la carte de routes configurée :

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name : le nom de la carte de routage qui sera annoncée si les conditions de la carte existante ou inexistante sont remplies.
- exist-map map name : le nom de la carte existante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- non-exist-map map name : le nom de la carte inexistante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- (Facultatif) check all paths : active la vérification de tous les chemins par la carte existante avec un préfixe dans le tableau BGP.

Étape 15 Supprimez les numéros de système autonome privés des mises à jour de routage sortant :

neighbor {ip-address} remove-private-as

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

Étape 16 Définissez les minuteries pour un homologue ou un groupe d'homologues BGP spécifique.

neighbor {ip-address} timers keepalive holdtime min holdtime

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive : la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive à son homologue. La valeur par défaut est de 60 secondes. Les valeurs valides sont comprises entre 0 et 65 535.
- holdtime : 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 de 180 secondes.
- min holdtime : 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 17 Activez l'authentification Message Digest 5 (MD5) sur une connexion TCP entre deux homologues BGP :

neighbor {ip-address} password string

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

La chaîne d'argument est un mot de passe sensible à la casse pouvant comporter jusqu'à 25 caractères lorsque la commande de 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.

Remarque
Lorsque vous définissez le premier caractère du mot de passe comme un nombre, ne fournissez pas d'espace immédiatement après le nombre. En d'autres termes, vous ne pouvez pas spécifier de mot de passe au format number-space-anything. L'espace après le numéro peut faire échouer l'authentification.

Étape 18 Précisez que les attributs de communautés doivent être envoyés à un voisin BGP :

neighbor {ip-address} send-community

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

Étape 19 Configurez le routeur comme prochain saut pour un voisin ou un groupe d'homologues utilisant BGP :

neighbor {ip-address}next-hop-self

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

Étape 20 Acceptez et tentez des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement :

neighbor {ip-address} ebgp-multihop [ttl]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

L'argument ttl spécifie la durée de vie dans une plage comprise entre 1 et 255 sauts.

Étape 21 Désactivez la vérification de connexion pour établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour :

neighbor {ip-address} disable-connected-check

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

Étape 22 Sécurisez une session d'homologation BGP et configurez le nombre maximum de sauts qui séparent deux homologues BGP (eBGP) externes :

neighbor {ip-address} ttl-security hops hop-count

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

L'argument hop-count est le nombre de sauts qui séparent les homologues eBGP. La valeur de la TTL est calculée par le routeur à partir de l'argument hop-count configuré. Les valeurs valides sont comprises entre 1 et 254.

Étape 23 Attribuez une pondération à une connexion de voisin :

neighbor {ip-address} weight number

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

Le numéro d'argument est la pondération à attribuer à une connexion de voisin. Les valeurs valides sont comprises entre 0 et 65 535.

Étape 24 Configurez l'ASA pour accepter uniquement une version BGP particulière :

neighbor {ip-address} version number

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

Le numéro d'argument spécifie le numéro de version du BGP. 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 25 Activez une option de session de transport TCP pour une session BGP :

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode : le type de connexion (active ou passive).
- path-mtu-discovery : active la découverte de l'unité de transfert maximale (MTU) du chemin de transport TCP. La découverte MTU du chemin TCP est activée par défaut.
- (Facultatif) disable : désactive la découverte MTU du chemin TCP.

Étape 26 Personnalisez l'attribut AS_PATH pour les routes reçues d'un voisin externe du protocole de passerelle frontière (eBGP) :

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (Facultatif) autonomous-system-number : le numéro d'un système autonome à ajouter au début de l'attribut AS_PATH. La plage de valeurs pour cet argument est tout numéro de système autonome valide compris entre 1 et 4294967295 ou 1.0 à XX.YY.
- (Facultatif) no-prepend : n'ajoute pas le numéro de système autonome local à aucune route reçue du voisin eBGP.

Étape 27 Pour mettre à jour une interface en tant que source pour un voisinage BGP :

neighbor *ip_address* **update-source** *interface_name*

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 update-source loop1
```

L'argument *interface_name* est le nom de l'interface que le voisin BGP utilise comme source pour le routage BGP.

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.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Précisez les réseaux à annoncer par les processus de routage de BGP :

network {network-number [mask network-mask]}[route-map map-tag]

Exemple :

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

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

- network-number : le réseau que BGP annoncera.
- (Facultatif) network-mask : le masque de réseau ou de sous-réseau avec l'adresse de masque.

- (Facultatif) map-tag : l'identifiant d'une carte de routage configurée. Il faut examiner la carte de routage pour filtrer les réseaux à annoncer. S'ils ne sont pas spécifiés, tous les réseaux sont annoncés.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Redistribuez les routes d'un autre domaine de routage dans un système autonome BGP :

redistribute protocol [process-id] [metric] [route-map [map-tag]]

Exemple :

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol : le protocole source à partir duquel les routes sont redistribuées. Il peut s'agir de l'une des options suivantes : Connected (connecté), EIGRP, OSPF, RIP ou Static (statique).
- (Facultatif) process-id : un nom pour le processus de routage spécifique.
- (Facultatif) metric : la mesure pour la route redistribuée.
- (Facultatif) map-tag : l'identifiant d'une carte de routage configurée.

Remarque

Il faut examiner la carte de routage pour filtrer les réseaux à redistribuer. S'ils ne sont pas spécifiés, tous les réseaux sont redistribués.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Configurez l'injection conditionnelle de routes pour injecter des routes plus précises dans une table de routage de BGP :

bgp inject-map inject-map exist-map exist-map [copy-attributes]

Exemple :

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map : le nom de la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale.
- exist-map : le nom de la carte de routage contenant les préfixes que le locuteur BGP suivra.
- (Facultatif) copy-attributes : configure la route injectée pour hériter des attributs de la route agrégée.

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 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Étape 3 Configurez la distance administrative des routes BGP :

distance bgp external-distance internal-distance local-distance

Exemple :

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance : distance administrative pour les routes BGP externes. Les routes sont externes lorsqu'elles sont apprises à partir d'un système autonome externe. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- internal-distance : distance administrative pour les routes BGP internes. Les routes sont internes lorsqu'elles sont apprises de l'homologue dans le système autonome local. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- local-distance : distance administrative pour les routes BGP locales. Les routes locales sont les réseaux répertoriés avec une commande de configuration de routeur de réseau, souvent comme portes dérobées, pour le routeur ou pour les réseaux qui sont redistribués à partir d'un autre processus. La plage de valeurs pour cet arguments est comprise entre 1 et 255.

Étape 4 (Facultatif) Configurez un processus de routage BGP pour distribuer une route par défaut (réseau 0.0.0.0) :

default-information originate

Étape 5 (Facultatif) Supprimez l'annonce des routes qui ne sont pas installées dans la base d'informations de routage (RIB) :

bgp suppress-inactive

Étape 6 Synchronisez le BGP avec votre système IGP (protocole de passerelle intérieure) :

synchronisation

Étape 7 Configurez la redistribution iBGP dans un IGP, tel que OSPF :

bgp redistribute-internal

Étape 8 Configurez des intervalles d'analyse des routeurs BGP pour la validation du saut suivant :

bgp scan-time scanner-interval

Exemple :

```
ciscoasa(config-router-af)# bgp scan-time 15
```

Valeurs valides pour l'argument d'intervalle d'analyse de 5 à 60 secondes. La valeur par défaut est de 60 secondes.

Étape 9 Contrôlez le nombre maximum de routes iBGP parallèles qui peuvent être installées dans une table de routage :

maximum-paths {number_of_paths|ibgp number_of_paths}

Exemple :

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Les valeurs valides pour l'argument number_of_paths sont comprises entre 1 et 8.

Si le mot clé ibgp n'est pas utilisé, l'argument number_of_paths contrôle le nombre maximum de routes EBGP parallèles.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 unicast

Étape 3 Créez une entrée agrégée dans une base de données BGP :

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

Exemple :

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address : l'adresse IPv6 agrégée.
- (Facultatif) as-set : génère des renseignements sur le chemin de définition du système autonome.
- (Facultatif) summary-only : filtre toutes les routes plus spécifiques à partir des mises à jour.
- (Facultatif) suppress-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes à supprimer.
- (Facultatif) advertise-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes afin de créer les communautés d'origine AS_SET.
- (Facultatif) attribute-map map-name : spécifie le nom de la carte de routage utilisée pour définir l'attribut de la route agrégée.

Étape 4 Définissez l'intervalle auquel les routes BGP seront agrégées :

bgp aggregate-timer seconds

Exemple :

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

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 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Étape 3 Ajoutez une entrée au tableau de voisins BGP :

neighbor ipv6-address remote-as autonomous-number

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

L'argument ipv6-address spécifie l'adresse IPv6 du prochain saut qui peut être utilisé pour atteindre le réseau spécifié. L'adresse IPv6 du prochain saut ne doit pas être connectée directement; une récursivité est effectuée pour trouver l'adresse IPv6 du saut suivant directement connecté. Lorsqu'un type d'interface et un numéro d'interface sont spécifiés, vous pouvez éventuellement spécifier l'adresse IPv6 du prochain saut vers lequel les paquets sont sortants. Vous devez préciser un type d'interface et un numéro d'interface lors de l'utilisation d'une adresse Link-Local comme prochain saut (le prochain saut de Link-Local doit également être un appareil adjacent).

Remarque
Cet argument doit être dans la forme documentée dans la RFC 2373, où l'adresse est spécifiée en hexadécimal en utilisant des valeurs de 16 bits entre les deux-points.

Étape 4 (Facultatif) Désactivez un groupe de voisins ou d'homologues :

neighbor ipv6-address shutdown

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

Étape 5 Échangez des renseignements avec un voisin BGP :

neighbor ipv6-address activate

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

Étape 6 Activez ou désactivez la fonctionnalité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin BGP :

neighbor {ip-address} ha-mode graceful-restart [disable]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 ha-mode graceful-restart
```

(Facultatif) Le mot clé disable désactive la fonctionnalité de redémarrage progressif du BGP pour un voisin.

Étape 7 Appliquez une carte de routage aux routes entrantes ou sortantes :

neighbor {ipv6-address} route-map map-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

Le mot clé dans applique une carte de routage aux routes entrantes.

Le mot clé out applique une carte de routage aux routes sortantes.

Étape 8 Distribuez les renseignements sur le voisin BGP comme spécifiés dans une liste de préfixes :

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

Le mot clé in implique que la liste de préfixes soit appliquée aux annonces entrantes de ce voisin.

Le mot clé out implique que la liste de préfixes soit appliquée aux annonces sortantes de ce voisin.

Étape 9 Configurez une liste de filtres :

neighbor {ipv6-address} filter-list access-list-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name : spécifie le numéro d'une liste d'accès de chemin au système autonome. Vous définissez cette liste d'accès avec la commande ip as-path access-list.
- in : signifie que la liste d'accès est appliquée aux annonces entrantes de ce voisin.
- out : signifie que la liste d'accès est appliquée aux annonces sortantes vers ce voisin.

Étape 10 Contrôlez le nombre de préfixes pouvant être reçus d'un voisin.

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum : le nombre maximum de préfixes autorisés pour ce voisin.
- (Facultatif) threshold : entier indiquant à quel pourcentage du maximum le routeur commence à générer un message d'avertissement. La plage se situe entre 1 et 100; la valeur par défaut est de 75 (pour cent).
- (Facultatif) restart interval : valeur entière (en minutes) qui spécifie l'intervalle de temps après lequel le voisin BGP redémarre.
- (Facultatif) warning-only : permet au routeur de générer un message de journal lorsque le nombre maximum de préfixes est dépassé, au lieu de mettre fin à l'homologation.

Étape 11 Autorisez un haut-parleur BGP (le routeur local) à envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut :

neighbor {ipv6-address} default-originate [route-map map-name]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

L'argument map-name est le nom de la carte de routage. La carte de routage permet l'injection conditionnelle de la route 0.0.0.0.

Étape 12 Définissez l'intervalle minimum entre l'envoi des mises à jour de routage BGP :

neighbor {ipv6-address} advertisement-interval seconds

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

L'argument seconds est le temps (en secondes). Les valeurs valides sont comprises entre 0 et 600.

Étape 13 Supprimez les numéros de système autonome privés des mises à jour de routage sortant :

neighbor {ipv6-address} remove-private-as

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

Étape 14 Annoncez les routes dans le tableau BGP qui correspondent à la carte de routes configurée :

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name : le nom de la carte de routage qui sera annoncée si les conditions de la carte existante ou inexistante sont remplies.
- exist-map map name : le nom de la carte existante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- non-exist-map map name : le nom de la carte inexistante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- (Facultatif) check all paths : active la vérification de tous les chemins par la carte existante avec un préfixe dans le tableau BGP.

Étape 15 Définissez les minuteries pour un homologue ou un groupe d'homologues BGP spécifique.

neighbor {ipv6-address} timers keepalive holdtime min holdtime

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive : la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive à son homologue. La valeur par défaut est de 60 secondes. Les valeurs valides sont comprises entre 0 et 65 535.

- holdtime : 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 de 180 secondes.
- min holdtime : 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 16 Activez l'authentification Message Digest 5 (MD5) sur une connexion TCP entre deux homologues BGP :

neighbor {ipv6-address} password string

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

La chaîne d'argument est un mot de passe sensible à la casse pouvant comporter jusqu'à 25 caractères lorsque la commande de 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.

Remarque
Lorsque vous définissez le premier caractère du mot de passe comme un nombre, ne fournissez pas d'espace immédiatement après le nombre. En d'autres termes, vous ne pouvez pas spécifier de mot de passe au format number-space-anything. L'espace après le numéro peut faire échouer l'authentification.

Étape 17 Précisez que les attributs de communautés doivent être envoyés à un voisin BGP :

neighbor {ipv6-address} send-community [standard]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

(Facultatif) mot clé standard : seules les communautés standard seront envoyées.

Étape 18 Configurez le routeur comme prochain saut pour un voisin ou un groupe d'homologues utilisant BGP :

neighbor {ipv6-address}next-hop-self

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

Étape 19 Acceptez et tentez des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement :

neighbor {ipv6-address} ebgp-multihop [ttl]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

L'argument ttl spécifie la durée de vie dans une plage comprise entre 1 et 255 sauts.

Étape 20 Désactivez la vérification de connexion pour établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour :

neighbor {ipv6-address} disable-connected-check

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

Étape 21 Sécurisez une session d'homologation BGP et configurez le nombre maximum de sauts qui séparent deux homologues BGP (eBGP) externes :

neighbor {ipv6-address} ttl-security hops hop-count

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

L'argument hop-count est le nombre de sauts qui séparent les homologues eBGP. La valeur de la TTL est calculée par le routeur à partir de l'argument hop-count configuré. Les valeurs valides sont comprises entre 1 et 254.

Étape 22 Attribuez une pondération à une connexion de voisin :

neighbor {ipv6-address} weight number

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

Le numéro d'argument est la pondération à attribuer à une connexion de voisin. Les valeurs valides sont comprises entre 0 et 65 535.

Étape 23 Configurez l'ASA pour accepter uniquement une version BGP particulière :

neighbor {ipv6-address} version number

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

Le numéro d'argument spécifie le numéro de version du BGP. La valeur par défaut est la version 4. Actuellement, seule la version 4 de BGP est prise en charge.

Étape 24 Activez une option de session de transport TCP pour une session BGP :

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode : le type de connexion (active ou passive).
- path-mtu-discovery : active la découverte de l'unité de transfert maximale (MTU) du chemin de transport TCP. La découverte MTU du chemin TCP est activée par défaut.

- (Facultatif) disable : désactive la découverte MTU du chemin TCP.

Étape 25 Personnalisez l'attribut AS_PATH pour les routes reçues d'un voisin externe du protocole de passerelle frontière (eBGP) :

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (Facultatif) autonomous-system-number : le numéro d'un système autonome à ajouter au début de l'attribut AS_PATH. La plage de valeurs pour cet argument est tout numéro de système autonome valide compris entre 1 et 4294967295 ou 1.0 à XX.YY.
- (Facultatif) no-prepend : n'ajoute pas le numéro de système autonome local à aucune route reçue du voisin eBGP.

  Mise en garde
  BGP ajoute au début le numéro de système autonome de chaque réseau BGP qu'une route traverse pour conserver les renseignements sur l'accessibilité du réseau et pour éviter les boucles de routage. Cette commande ne doit être configurée que pour la migration du système autonome et doit être supprimée une fois la transition terminée. Cette procédure ne doit être tentée que par un opérateur de réseau expérimenté. Des boucles de routage peuvent être créées par une configuration inadéquate.

Étape 26 Pour mettre à jour une interface en tant que source pour le voisinage BGP :

neighbor {ipv6-address} update-source {interface name}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 update-source loop1
```

L'argument interface name spécifie le nom de l'interface que le voisin BGP utilise comme source pour le routage BGP.

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.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp *autonomous-num*

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Étape 3 Précisez les réseaux à annoncer par les processus de routage de BGP :

network {*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] | *ipv6_prefix*/*prefix_length*} [**route-map** *route_map_name*]

Exemple :

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
ciscoasa(config-router-af)# network outside-prefix 1::/64
ciscoasa(config-router-af)# network outside-prefix 2::/64
```

- *prefix_delegation_name* : si vous activez le client de délégation de préfixe DHCPv6 (**ipv6 dhcp client pd**), vous pouvez annoncer le ou les préfixes. Pour faire figurer dans un sous-réseau le préfixe, spécifiez *subnet_prefix*/*prefix_length*.
- *ipv6 network*/*prefix_length* : le réseau que BGP annoncera.
- (Facultatif) **route-map** *name* : l'identifiant d'une carte de routage configurée. Il faut examiner la carte de routage pour filtrer les réseaux à annoncer. S'ils ne sont pas spécifiés, tous les réseaux sont annoncés.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

Étape 3 Redistribuez les routes d'un autre domaine de routage dans un système autonome BGP :

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

Exemple :

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol : le protocole source à partir duquel les routes sont redistribuées. Il peut s'agir de l'une des options suivantes : Connected (connecté), EIGRP, OSPF, RIP ou Static (statique).
- (Facultatif) process-id : pour le protocole ospf, il s'agit d'un ID de processus OSPF approprié à partir duquel les routes doivent être redistribuées. Cela identifie le processus de routage. Cette valeur prend la forme d'un nombre décimal différent de zéro.

  Remarque
  Cette valeur est renseignée automatiquement pour les autres protocoles.

- (Facultatif) metric metric value : lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même routeur, la mesure sera transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée. La valeur par défaut est 0.
- (Facultatif) match internal | external1 | external2 | NSSA external 1 | NSSA external 2 : pour les critères selon lesquels les routes OSPF sont redistribuées dans d'autres domaines de routage. Les choix sont les suivants :
  - internal : routes internes à un système autonome spécifique.
  - external 1 : routes externes au système autonome, mais importées dans BGP en tant que route externe OSPF de type 1.
  - external 2 : routes externes au système autonome, mais importées dans BGP en tant que route externe OSPF de type 2.
  - NSSA external 1 : routes externes au système autonome, mais importées dans BGP en tant que routes externes OSPF NSSA de type 1.
  - NSSA external 2 : routes externes au système autonome, mais importées dans BGP en tant que routes externes OSPF NSSA de type 2.
- (Facultatif) map-tag : l'identifiant d'une carte de routage configurée.

Remarque
Il faut examiner la carte de routage pour filtrer les réseaux à redistribuer. S'ils ne sont pas spécifiés, tous les réseaux sont redistribués.

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 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

Étape 3 Configurez l'injection conditionnelle de routes pour injecter des routes plus précises dans une table de routage de BGP :

bgp inject-map inject-map exist-map exist-map [copy-attributes]

Exemple :

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map : le nom de la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale.
- exist-map : le nom de la carte de routage contenant les préfixes que le locuteur BGP suivra.
- (Facultatif) copy-attributes : configure la route injectée pour hériter des attributs de la route agrégée.

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 :

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

  Affiche les entrées de la table de routage BGP.

- **show bgp** cidr-only

  Affiche les routes avec des masques réseau non naturels (c'est-à-dire le routage inter-domaine sans classe ou CIDR).

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  Affiche les routes qui appartiennent aux communautés BGP spécifiées.

- **show bgp community-list community-list-name [exact-match]**

  Affiche les routes autorisées par la liste de communautés BGP.

- **show bgp filter-list** *access-list-number*

  Affiche les routes conformes à une liste de filtres spécifiée.

- **show bgp injected-paths**

  Affiche tous les chemins injectés dans la table de routage BGP.

- **show bgp ipv4 unicast**

  Affiche les entrées de la table de routage BGP d'IP version 4 (IPv4) pour les sessions de monodiffusion.

- show bgp ipv6 unicast

  Affiche les entrées de la table de routage du protocole de passerelle frontière (BGP) IPv6.

- show bgp ipv6 community

  Affiche les routes qui appartiennent aux communautés du protocole de passerelle frontière (BGP) IPv6 spécifiées.

- show bgp ipv6 community-list

  Affiche les routes autorisées par la liste de communautés du protocole de passerelle frontière (BGP) IPv6.

- show bgp ipv6 filter-list

  Affiche les routes conformes à une liste de filtres IPv6 spécifiée.

- show bgp ipv6 inconsistent-as

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 dont les systèmes autonomes sont incohérents.

- show bgp ipv6 neighbors

  Affiche des renseignements sur les connexions du protocole de passerelle frontière (BGP) IPv6 aux voisins.

- show bgp ipv6 paths

  Affiche tous les chemins du protocole de passerelle frontière (BGP) IPv6 dans la base de données.

- show bgp ipv6 prefix-list

Affiche les routes qui correspondent à une liste de préfixes.

- show bgp ipv6 quote-regexp

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 correspondant à l'expression régulière du chemin d'accès au système autonome sous la forme d'une chaîne de caractères entre guillemets.

- show bgp ipv6 regexp

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 correspondant à l'expression régulière du chemin d'accès au système autonome.

- show bgp ipv6 route-map

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 qui n'ont pas pu être installées dans la table de routage.

- show bgp ipv6 summary

  Affiche l'état de toutes les connexions du protocole de passerelle frontière (BGP) IPv6.

- show bgp neighbors ip_address

  Affiche des renseignements sur les connexions BGP et TCP à des voisins.

- show bgp paths [LINE]

  Affiche tous les chemins BGP dans la base de données.

- show bgp pending-prefixes

  Affiche les préfixes qui sont en attente de suppression.

- show bgp prefix-list prefix_list_name [WORD]

  Affiche les routes qui correspondent à une liste de préfixes spécifiée.

- show bgp regexp regexp

  Affiche les routes qui correspondent à l'expression régulière du chemin d'accès au système autonome.

- show bgp replication [index-group | ip-address]

  Affiche les statistiques de réplication de mise à jour pour les groupes de mise à jour du BGP.

- show bgp rib-failure

  Affiche les routes BGP qui n'ont pas pu être installées dans le tableau de la base d'information de routage (RIB).

- show bgp route-map map-name

  Affiche les entrées de la table de routage BGP, en fonction de la carte de routage spécifiée.

- show bgp summary

  Affiche l'état de toutes les connexions BGP.

- show bgp system-config

  Affiche la configuration BGP spécifique au contexte système en mode de contexte multiple.

  Cette commande est disponible dans tous les contextes utilisateur en mode de contexte multiple.

- show bgp update-group

  Affiche des renseignements sur les groupes de mise à jour du BGP.

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.

Exemple de BGP

Cet exemple montre comment activer et configurer BGPv4 avec différents processus facultatifs.

1. Définissez les conditions pour la redistribution des routes d'un protocole de routage vers un autre protocole de routage, ou activez le routage par politique :

   ```
   ciscoasa(config)# route-map mymap2 permit 10
   ```

2. Redistribuez toutes les routes qui ont une adresse de route ou un paquet correspondant à une des listes d'accès spécifiées :

   ```
   ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
   ```

3. Indiquez où obtenir les paquets qui transmettent une clause de correspondance d'une carte de routage pour le routage des politiques :

   ```
   ciscoasa(config-route-map)# set ip next-hop peer address
   ```

4. Activez un processus de routage BGP à partir du mode de configuration global :

   ```
   ciscoasa(config)# router bgp 2
   ```

5. Configurez un ID de routeur fixe pour le processus de routage du protocole BGP (Border Gateway Protocol) local dans le mode de configuration de la famille d'adresses :

   ```
   ciscoasa(config)# address-family ipv4
   ciscoasa(config-router-af)# bgp router-id 19.168.254.254
   ```

6. Ajoutez une entrée au tableau de voisins BGP :

   ```
   ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
   ```

7. Appliquez une carte de routage aux routes entrantes ou sortantes :

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

8. Mettez à jour une interface en tant que source d'un voisin prenant en charge le protocole BGP :

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 update-source loop1
```

Cet exemple montre comment activer et configurer BGPv6 avec différents processus facultatifs.

1. Définissez les conditions pour la redistribution des routes d'un protocole de routage vers un autre protocole de routage, ou activez le routage par politique :

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. Redistribuez toutes les routes qui ont une adresse de route ou un paquet correspondant à une des listes d'accès spécifiées :

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. Indiquez où obtenir les paquets qui transmettent une clause de correspondance d'une carte de routage pour le routage des politiques :

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. Activez un processus de routage BGP à partir du mode de configuration global :

```
ciscoasa(config)# router bgp 2
```

5. Configurez un ID de routeur fixe pour le processus de routage du protocole BGP (Border Gateway Protocol) local dans le mode de configuration de la famille d'adresses :

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

```
address-family ipv6 [unicast]
```

7. Ajoutez une entrée au tableau de voisins BGP :

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. Appliquez une carte de routage aux routes entrantes ou sortantes :

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

9. Mettez à jour une interface en tant que source d'un voisin prenant en charge le protocole BGP :

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 update-source loop1
```

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 commandes suivantes : **router bgp, bgp maxas-limit, bgp log-neighbor-changes, bgp transport path-mtu-discovery, bgp fast-external-fallover, bgp enforce-first-as, bgp asnotation dot, timers bgp, bgp default local-preference, bgp always-compare-med, bgp bestpath compare-routerid, bgp deterministic-med, bgp bestpath med missing-as-worst, policy-list, match as-path, match community, match metric, match tag, as-path access-list, community-list, address-family ipv4, bgp router-id, distance bgp, table-map, bgp suppress-inactive, bgp redistribute-internal, bgp scan-time, bgp nexthop, aggregate-address, neighbor, bgp inject-map, show bgp, show bgp cidr-only, show bgp all community, show bgp all neighbors, show bgp community, show bgp community-list, show bgp filter-list, show bgp injected-paths, show bgp ipv4 unicast, show bgp neighbors, show bgp paths, show bgp pending-prefixes, show bgp prefix-list, show bgp regexp, show bgp replication, show bgp rib-failure, show bgp route-map, show bgp summary, show bgp system-config, show bgp update-group, clear route network, maximum-path, network.** Nous avons modifié les commandes suivantes : **show route**, **show route summary**, **show running-config router**, **clear config router**, **clear route all**, **timers lsa arrival**, **timers pacing**, **timers throttle**, **redistribute bgp**.
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 introduit la commande suivante : bgp router-id clusterpool
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 introduit les commandes suivantes : bgp graceful-restart, neighbor ha-mode graceful-restart

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP pour les cartes annoncées	9.3(1)	Nous avons ajouté la prise en charge des cartes annoncées BGPv4. Nous avons introduit la commande suivante : neighbor advertise-map
Prise en charge BGP pour IPv6	9.3(2)	Nous avons ajouté la prise en charge d'IPv6. Nous avons introduit les commandes suivantes : address-family ipv6, ipv6 prefix-list, ipv6 prefix-list description, ipv6 prefix-list sequence-number, match ipv6 next-hop, match ipv6 route-source, match ipv6- address prefix-list, set ipv6-address prefix -list, set ipv6 next-hop, set ipv6 next-hop peer-address Nous avons modifié la commande suivante : bgp router-id
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 la commande suivante : **network**
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**
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.