OSPF

Ce chapitre décrit comment configurer défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage OSPF (Open Shortest Path First).

OSPF

Ce chapitre décrit comment configurer défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage OSPF (Open Shortest Path First).

À propos d'OSPF

OSPF est un protocole de routage de passerelle intérieure qui utilise des états de liaison plutôt que des vecteurs de distance pour la sélection de chemin. OSPF propage des publicités d'état de liens plutôt que des mises à jour de la table de routage. Comme seuls les LSA sont échangés au lieu des tableaux de routage complets, les réseaux OSPF convergent plus rapidement que les réseaux IPS.

OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

Les avantages d'OSPF par rapport à RIP sont les suivants :

- Les mises à jour de la base de données d'états de liens OSPF sont envoyées moins fréquemment que les mises à jour RIP, et la base de données d'états de liens est mise à jour instantanément, plutôt que lentement, à mesure que les informations périmées expirent.
- Les décisions de routage sont basées sur le coût, qui est une indication du surdébit nécessaire pour envoyer des paquets sur une certaine interface. appareil de défense contre les menaces calcule le coût d'une

interface en fonction de la bande passante du lien plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour préciser les chemins privilégiés.

L'inconvénient des algorithmes du chemin le plus court d'abord est qu'ils nécessitent beaucoup de cycles du processeur et de mémoire.

L'appareil de défense contre les menaces peut exécuter deux processus du protocole OSPF simultanément sur différents ensembles d'interfaces. Vous pourriez souhaiter exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (la NAT permet à ces interfaces de coexister, mais OSPF ne permet pas le chevauchement d'adresses). Ou vous pouvez exécuter un processus à l'intérieur et un autre à l'extérieur et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer les routages dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage IP ou de routes statiques et connectées configurées sur des interfaces activées pour OSPF.

appareil de défense contre les menaces prend en charge les fonctionnalités OSPF suivantes :

- Routages intra-zones, inter-zones et externes (type I et type II).
- Liens virtuels.
- Inondation de LSA.
- Authentification pour les paquets OSPF (authentification par mot de passe et authentification MD5).
- Configuration de appareil de défense contre les menaces en tant que routeur désigné ou routeur de secours désigné L'appareil de défense contre les menaces peut également être configuré comme un ABR.
- Zones tampons et zones tampons.
- Routeur de frontière de zone, filtrage LSA de type 3

OSPF prend en charge MD5 et l'authentification du voisin en texte clair. L'authentification doit être utilisée avec tous les protocoles de routage lorsque cela est possible, car la redistribution de routage entre OSPF et d'autres protocoles (comme RIP) peut être utilisée par les attaquants pour détourner des informations de routage.

Si la NAT est utilisée, si OSPF fonctionne sur des zones publiques et privées, et si le filtrage d'adresses est requis, vous devez exécuter deux processus OSPF, un pour les zones publiques et un pour les zones privées.

Un routeur qui a des interfaces dans plusieurs zones est appelé routeur de frontière de zone (ABR). Un routeur qui agit comme une passerelle pour redistribuer le trafic entre les routeurs utilisant OSPF et les routeurs utilisant d'autres protocoles de routage est appelé un routeur de frontière de système autonome (ASBR).

Un ABR utilise des LSA pour envoyer des informations sur les routes disponibles à d'autres routeurs OSPF. Le filtrage du LSA ABR de type 3 vous permet d'avoir des zones privée et publique distinctes, l'ASA agissant comme un ABR. Les LSA de type 3 (routes inter-zones) peuvent être filtrées d'une zone à une autre, ce qui vous permet d'utiliser la NAT et l'OSPF ensemble sans annoncer de réseaux privés.

Remarque Seuls les LSA de type 3 peuvent être filtrés. Si vous configurez l'appareil de défense contre les menaces comme ASBR dans un réseau privé, il enverra des LSA de type 5 décrivant les réseaux privés, qui seront inondés à l'ensemble du système autonome, y compris les zones publiques.

Si la NAT est utilisée, mais OSPF n'est exécuté que dans les zones publiques, les routages vers les réseaux publics peuvent être redistribués à l'intérieur du réseau privé, soit par défaut, soit comme LSA externes de type AS externes. Cependant, vous devez configurer des routes statiques pour les réseaux privés protégés par appareil de défense contre les menaces . De plus, vous ne devez pas combiner réseaux publics et réseaux privés sur la même interface appareil de défense contre les menaces .

Vous pouvez avoir deux processus de routage OSPF, un processus de routage RIP et un processus de routage EIGRP en même temps sur l'appareil de défense contre les menaces .

Prise en charge OSPF pour les paquets Fast Hello

La prise en charge OSPF des paquets Hello rapides offre un moyen de configurer l'envoi de paquets Hello à des intervalles inférieurs à une seconde. Une telle configuration accélérerait la convergence dans un réseau OSPF (Open Shortest Path First).

Conditions préalables à la prise en charge d'OSPF pour les paquets Fast Hello

OSPF doit déjà être configuré dans le réseau ou configuré en même temps que la fonction de prise en charge OSPF des paquets Fast Hello.

Intervalle Hello et intervalle mort OSPF

Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF pour maintenir la connectivité avec ces derniers. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet et de 30 secondes pour une liaison non diffusée. Les paquets Hello comprennent une liste de tous les voisins pour lesquels un paquet Hello a été reçu dans l'intervalle mort. L'intervalle mort est également un intervalle configurable (en secondes). Par défaut, il est quatre fois supérieur à la valeur de l'intervalle Hello. La valeur de tous les intervalles Hello doit être la même dans un réseau. De même, la valeur de tous les intervalles morts doit être la même dans un réseau.

Ces deux intervalles fonctionnent ensemble pour maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d'un voisin dans l'intervalle mort, il déclarera ce voisin en panne.

Paquets Fast Hello OSPF

Les paquets Hello OSPF rapides sont des paquets Hello envoyés à des intervalles de moins d'une seconde. Pour comprendre les paquets Hello rapides, vous devez déjà comprendre la relation entre les paquets Hello d'OSPF et l'intervalle mort. Consultez Intervalle Hello et intervalle mort OSPF, à la page 3.

Les paquets OSPF fast Hello sont obtenus à l'aide de la commande ospf dead-interval. L'intervalle mort est défini à 1 seconde et la valeur Hello-multiplier est définie sur le nombre de paquets Hello que vous souhaitez envoyer pendant cette 1 seconde, fournissant ainsi des paquets Hello inférieurs à la seconde ou « rapides ».

Lorsque des paquets Hello rapides sont configurés sur l'interface, l'intervalle Hello annoncé dans les paquets Hello envoyés par cette interface est réglé à 0. L'intervalle Hello dans les paquets Hello reçus sur cette interface est ignoré.

L'intervalle mort doit être cohérent sur un segment, qu'il soit défini à 1 seconde (pour les paquets Hello rapides) ou à une autre valeur. Le multiplicateur Hello n'a pas besoin d'être le même pour tout le segment tant qu'au moins un paquet Hello est envoyé dans l'intervalle mort.

Avantages des paquets Fast Hello OSPF

L’avantage de la fonctionnalité OSPF Fast Hello Packets est que votre réseau OSPF connaîtra un temps de convergence plus rapide que sans les paquets rapides Hello. Cette fonctionnalité vous permet de détecter les voisins perdus en moins d’une seconde. Elle est particulièrement utile dans les segments de réseau local, où la perte de voisin peut ne pas être détectée par la couche physique et la couche de liaison de données de l’Open System Interconnection (OSI).

Différences d'implémentation entre OSPFv2 et OSPFv3

OSPFv3 n'est pas rétrocompatible avec OSPFv2. Pour utiliser OSPF en vue d’acheminer le trafic IPv4 et IPv6, vous devez exécuter simultanément OSPFv2 et OSPFv3. Ils coexistent, mais n’interagissent pas entre eux.

Les fonctionnalités supplémentaires fournies par OSPFv3 sont les suivantes :

- Traitement du protocole par liaison
- Suppression de la sémantique d’adressage.
- Ajout de la portée de submersion.
- Prise en charge de plusieurs instances par lien.
- Utilisation de l’adresse locale de lien IPv6 pour la découverte de voisin et d’autres fonctionnalités.
- Les LSA sont exprimées en tant que préfixe et longueur de préfixe.
- Ajout de deux types de LSA.
- Gestion des types de LSA inconnus
- Prise en charge de l’authentification par la norme IPsec ESP pour le trafic de protocole de routage OSPFv3, comme le spécifie la RFC 4552.

Exigences et conditions préalables OSPF

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Directives pour OSPF

Directives sur le mode pare-feu

OSPF ne prend en charge que le mode pare-feu routé. OSPF ne prend pas en charge le mode de pare-feu transparent.

Directives High Availability (haute disponibilité)

OSPFv2 et OSPFv3 prennent en charge les High Availability (haute disponibilité) sans état.

Directives IPv6

- OSPFv2 ne prend pas en charge IPv6.
- OSPFv3 prend en charge IPv6.
- OSPFv3 utilise IPv6 pour l'authentification.
- L'appareil de défense contre les menaces installe les routages OSPFv3 dans le RIB IPv6, à condition qu'il s'agisse du meilleur routage.

Paquets Hello OSPFv3 et GRE

En règle générale, le trafic OSPF ne passe pas par le tunnel GRE. Lorsqu'OSPFv3 sur IPv6 est encapsulé à l'intérieur de GRE, la validation de l'en-tête IPv6 pour les vérifications de sécurité telles que la destination de multidiffusion échoue. Le paquet est abandonné en raison de la validation de vérification de sécurité implicite, car ce paquet a une multidiffusion IPv6 de destination.

Vous pouvez définir une règle de préfiltre pour contourner le trafic GRE. Cependant, avec la règle de préfiltre, les paquets internes ne seraient pas interrogés par le moteur d'inspection.

Directives de mise en grappe

- Le chiffrement OSPFv3 n'est pas pris en charge. Un message d'erreur s'affiche si vous essayez de configurer le chiffrement OSPFv3 dans un environnement de mise en grappe.
- En mode d'interface étendue, le routage dynamique n'est pas pris en charge sur les interfaces de gestion uniquement.
- En mode d'interface individuel, veillez à définir les unités de contrôle et de données comme des voisins OSPFv2 ou OSPFv3.
- En mode d'interface individuelle, les contiguïtés OSPFv2 ne peuvent être établies qu'entre deux contextes sur une interface partagée sur l'unité de contrôle. La configuration de voisins statiques est prise en charge uniquement sur les liaisons point à point; par conséquent, une seule instruction voisin est autorisée sur une interface.
- Lorsqu'un changement de rôle de contrôle se produit dans la grappe, le comportement suivant se produit :
    - En mode d'interface étendue, le processus du routeur est actif uniquement sur l'unité de contrôle et est à l'état suspendu sur les unités de données. Chaque unité de grappe a le même ID de routeur, car la configuration a été synchronisée à partir de l'unité de contrôle. Par conséquent, un routeur

voisin ne remarque aucun changement dans l'ID de routeur de la grappe lors d'un changement de rôle.

- En mode d'interface individuelle, le processus du routeur est actif sur toutes les unités de la grappe. Chaque unité de grappe choisit son propre ID de routeur dans l'ensemble de grappes configuré. Une modification du rôle de contrôle dans la grappe ne modifie en rien la topologie de routage.

Commutation multiprotocole par étiquette (MPLS) et directives OSPF

Lorsqu'un routeur configuré pour MPLS envoie des paquets de mise à jour d'état de liaison (LS) qui contiennent des publicités d'état de liaison (LSA) de type 10 couvrantes qui comprennent un en-tête MPLS, l'authentification échoue et le périphérique abandonne en mode silencieux les paquets de mise à jour plutôt que d'en accuser réception. Finalement, le routeur homologue mettra fin à la relation de voisin, car il n'a reçu aucun accusé de réception.

Assurez-vous que le transfert sans arrêt (NSF) est désactivé sur le périphérique pour que la relation de voisin reste stable :

- Accédez à la page **Transfert non stop** dans centre de gestion(**Périphériques** > **Gestion des périphériques (sélectionnez le périphérique souhaité)** > **Routage** > **OSPF** > **Avancé** > **Transfert non stop**).

  Assurez-vous que les cases sur la **capacité de transfert non stop** ne sont pas cochées.

Remarque Les modèles Firepower 4100/9300 peuvent avoir une latence élevée lors de l'utilisation de MPLS, car ils n'ont pas suffisamment d'équilibrage de la charge sur plusieurs files d'attente de réception.

Directives de redistribution de routage

- La redistribution des cartes de routage avec la liste de préfixes IPv4 ou IPv6 sur OSPFv2 ou OSPFv3 n'est pas prise en charge. Utilisez une liste d'accès dans la carte de routage sur OSPF pour la redistribution.
- Lorsqu'OSPF est configuré sur un périphérique qui fait partie du réseau EIGRP ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser la voie de routage (le protocole EIGRP ne prend pas encore en charge la balise de routage).

  Lors de la redistribution d'OSPF dans EIGRP et d'EIGRP dans OSPF, une boucle de routage se produit lorsqu'il y a une panne sur l'une des liaisons ou des interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives supplémentaires

- OSPFv2 et OSPFv3 prennent en charge plusieurs instances sur une interface.
- OSPFv3 prend en charge le chiffrement par le biais des en-têtes ESP dans un environnement sans grappe.
- OSPFv3 prend en charge le chiffrement sans charge utile.

- OSPFv2 prend en charge les mécanismes de redémarrages progressifs NSF de Cisco et IETF NSF tels que définis dans les RFC 4811, 4812 et 3623 respectivement.
- OSPFv3 prend en charge le mécanisme de redémarrage progressif tel que défini dans la RFC 5187.
- Il y a une limite au nombre de routages intra-zone (type 1) qui peuvent être distribués. Pour ces routes, un seul LSA de type 1 contient tous les préfixes. Comme le système a une limite de 35 Ko pour la taille des paquets, un paquet de 3 000 routages dépasse la limite. Considérez 2900 routes de type 1 comme le nombre maximal pris en charge.
- Pour un périphérique utilisant le routage virtuel, vous pouvez configurer OSPFv2 et OSPFv3 pour un routeur virtuel global. Cependant, vous ne pouvez configurer qu'OSPFv2 pour un routeur virtuel défini par l'utilisateur.
- 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.

Configurer le protocole OSPFv2

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv2. Pour un périphérique utilisant le routage virtuel, vous pouvez configurer OSPFv2 pour les routeurs virtuels mondiaux et définis par l'utilisateur.

Configurer les zones, les plages et les liens virtuels OSPF

Vous pouvez configurer plusieurs paramètres de zone OSPF, qui comprennent la définition de l'authentification, la définition des zones tampons et l'affectation de coûts spécifiques à la route récapitulative par défaut. Vous pouvez activer jusqu'à deux instances de processus OSPF. Chaque processus OSPF a ses propres zones et réseaux associés. L'authentification offre une protection par mot de passe contre l'accès non autorisé à une zone.

Les zones tampons sont des zones dans lesquelles les informations sur les routages externes ne sont pas envoyées. Au lieu de cela, une route externe par défaut est générée par l'ABR dans la zone tampon pour les destinations externes au système autonome. Pour tirer parti de la prise en charge de la zone tampon OSPF, le routage par défaut doit être utilisé dans la zone tampon.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Cochez la case du **processus 1**. Vous pouvez activer jusqu'à deux instances de processus OSPF pour chaque contexte/routeur virtuel. Vous devez choisir un processus OSPF pour pouvoir configurer les paramètres de la zone.

Si le périphérique utilise le routage virtuel, les champs d'ID affichent les ID de processus uniques générés pour le routeur virtuel choisi.

Étape 6 Choisissez le **rôle OSPF** dans la liste déroulante et saisissez une description dans le champ suivant. Les options sont Internal, ABR, ASBR et ABR et ASBR. Consultez À propos d'OSPF, à la page 1 pour obtenir une description des rôles OSPF.

Étape 7 Sélectionnez **Area** > **Add** (ajouter une zone intermédiaire).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 8 Configurez les options de zone suivantes pour chaque processus OSPF :

- **Processus OSPF** : Choisissez l'ID de processus. Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **Area ID** (ID de zone) : désignation de la zone pour laquelle les routages doivent être résumés.
- **Area Type** (type de zone) : choisissez l'une des options suivantes :
  - **Normal** : (par défaut) zone OSPF standard.
  - **Stub** : une zone tampon ne comporte aucun routeur ni de zone au-delà. Les zones tampons empêchent les LSA externes du système autonome (LSA de type 5) d'être submergées dans la zone tampon. Lorsque vous créez une zone tampon, vous pouvez empêcher les LSA récapitulatifs d'être submergés (types 3 et 4) dans la zone en NE cochant PAS la case **Summary Stub** (Tampon résumé).
  - **NSSA** : fait de la zone une zone moins dense (NSSA). Les contrats NSSA acceptent les LSA de type 7. Vous pouvez désactiver la redistribution de routage en NE cochant PAS la case **Redistribute** (Redistribuer) mais en cochant la case **Default Information Originate** (origine des informations par défaut). Vous pouvez empêcher l'inondation des LSA récapitulatifs dans la zone en NE cochant PAS la case **Summary NSSA** (NSSA récapitulatifs).
- **(Metric Value** (Valeur de la métrique) : la métrique utilisée pour générer la voie de routage par défaut. La valeur par défaut est 10. Les valeurs de métrique valides sont comprises entre 0 et 16777214.
- **Type de mesure** : Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.
- **Available network** (Réseau disponible) : choisissez un des réseaux disponibles et cliquez sur **Add**(ajouter), ou cliquez sur **Ajouter** ( ) pour ajouter un nouvel objet réseau. Consultez Réseau pour connaître la procédure d'ajout de réseaux.
- **Authentication** (authentification) : choisissez l'authentification OSPF :
  - **None** (Aucun) : (par défaut) Désactive l'authentification de zone OSPF.
  - **Password** (Mot de passe) : fournit un mot de passe en clair pour l'authentification de zone, ce qui n'est pas recommandé lorsque la sécurité est un problème.
  - **MD5** : permet l'authentification MD5.
- **Default Cost** (coût par défaut) : Le coût par défaut pour la zone OSPF, qui est utilisé pour déterminer les chemins les plus courts vers la destination. Les valeurs valides vont de 0 à 65 535. La valeur par défaut est 1.

Étape 9 Cliquez sur **OK** pour enregistrer la configuration de la zone.

Étape 10 Sélectionnez **Plage** > **Ajouter**.

- Choisissez l'un des réseaux disponibles et si vous souhaitez en faire la publicité, ou,
- cliquez sur **Ajouter** (+) pour ajouter un nouvel objet réseau. Consultez Réseau pour connaître la procédure d'ajout de réseaux.

Étape 11 Cliquez sur **OK** pour enregistrer la configuration de la plage.

Étape 12 Sélectionnez **Virtual Link** (liaison virtuelle), cliquez sur **Add** (+)(ajouter) et configurez les options suivantes pour chaque processus OSPF :

- **Peer Router** (routeur homologue) : Choisissez l'adresse IP du routeur homologue. Pour ajouter un nouveau routeur homologue, cliquez sur **Ajouter** (+). Consultez Réseau pour connaître la procédure d'ajout de réseaux.
- **Hello Interval** (intervalle Hello) : le temps en secondes entre les paquets Hello envoyés sur une interface. L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès sur un réseau spécifique. Les valeurs valides vont de 0 à 65 535. La valeur par défaut est 10.

  Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus le trafic acheminé sur l'interface est important.
- **Transmit Delay** (délai de transmission) : le temps estimée en secondes qui est nécessaire pour envoyer un paquet LSA sur l'interface. La valeur entière doit être supérieure à zéro. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 1.

  Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse.
- **Retransmit Interval** (Intervalle de retransmission) : le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. L'intervalle de retransmission est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 65 535. La valeur par défaut est égale à 5.

  Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles.
- **Dead Interval** (intervalle mort) : la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne. L'intervalle mort est un entier non signé. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 0 à 65 535.
- **Authentication** (authentification) : choisissez l'authentification par lien virtuel OSPF parmi les options suivantes :
  - **Aucun** : (par défaut) désactive l'authentification de zone de lien virtuel.

- **Authentification de zone** : active l'authentification de zone à l'aide de MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.
- **Mot de passe** : fournit un mot de passe en texte clair pour l'authentification par lien virtuel, ce qui n'est pas recommandé lorsque la sécurité est un problème.
- **MD5** : permet l'authentification MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.

  Remarque Assurez-vous de saisir uniquement des chiffres comme ID de clé MD5.
- **Chaîne de clé** : permet l'authentification par chaîne de clé. Cliquez sur **Add**(ajouter) et créez la chaîne de clés, puis cliquez sur **Save** (Enregistrer). Pour la procédure détaillée, consultez Création d'objets de chaîne de clé. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie.

Étape 13 Cliquez sur **OK** pour enregistrer la configuration du lien virtuel.

Étape 14 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Passez à Configurer la redistribution OSPF.

Configurer la redistribution OSPF

Le périphérique défense contre les menaces peut contrôler la redistribution des routes entre les processus de routage OSPF. Les règles de redistribution des routages d'un processus de routage vers un processus de routage OSPF sont affichées. Vous pouvez redistribuer les routages détectés par EIGRP, IPS et BGP dans le processus de routage OSPF. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage OSPF.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Dans la liste déroulante **Rôle OSPF**, choisissez le rôle .

Étape 6 Cliquez sur **Redistribution** > **Add (ajouter)**.

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 7 Configurez les options de redistribution suivantes pour chaque processus OSPF :

- **Processus OSPF** : Choisissez l'ID de processus. Pour un périphérique utilisant le routage virtuel, cette liste déroulante affiche les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **Route Type** (Type de route) : choisissez un des types suivants :
  - **Static** (statique) : redistribue les routes statiques vers le processus de routage OSPF.
  - **Connected** (Connecté) : redistribue les routes connectées (les routes sont établies automatiquement parce que l'adresse IP est activée sur l'interface) vers le processus de routage OSPF. Les routes connectées sont redistribuées en tant que routes externes vers le périphérique. Vous pouvez choisir d'utiliser des sous-réseaux dans la liste Facultatif.
  - **OSPF** : redistribue les routages d'un autre processus de routage OSPF, par exemple, interne, externe 1 et 2, NSSA externe 1 et 2, ou s'il faut utiliser des sous-réseaux. Vous pouvez sélectionner ces options dans la liste Facultatif.
  - **BGP** : redistribue les routes à partir du processus de routage BGP. Ajoutez le numéro de système autonome et si vous souhaitez utiliser des sous-réseaux.
  - **RIP** : redistribue les routes à partir du processus de routage RIP. Vous pouvez choisir d'utiliser des sous-réseaux dans la liste Facultatif.

    Remarque Comme un routeur virtuel défini par l'utilisateur ne prend pas en charge RIP, vous ne pouvez pas redistribuer les routages à partir de RIP.

  - **EIGRP** : redistribue les routes à partir du processus de routage EIGRP. Ajoutez le numéro de système autonome et si vous souhaitez utiliser des sous-réseaux.
- **Metric Value** (Valeur de la mesure) : valeur de la mesure pour les routages distribués. La valeur par défaut est 10. Les valeurs valides sont comprises entre 0 et 16 777214.

  Lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même périphérique, 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.
- **Type de mesure** : Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.
- **Tag value** (Valeur de balise) la balise spécifie la valeur décimale sur 32 bits associée à chaque routage externe qui n'est pas utilisé par OSPF lui-même, mais qui peut être utilisé pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides sont comprises entre 0 et 4294967295.
- **RouteMap** (carte de routage) : vérifie le filtrage de l'importation des routes du protocole de routage source au protocole de routage actuel. Si ce paramètre n'est pas spécifié, toutes les routes sont redistribuées. Si ce paramètre est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée. Vous pouvez aussi ajouter une nouvelle carte de routage en cliquant sur **Ajouter** (+). Consultez Configurer une entrée de carte de routage pour ajouter une nouvelle carte de routage.

Étape 8 Cliquez sur **OK** pour enregistrer la configuration de redistribution.

Étape 9 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer le filtrage inter-zones OSPF, à la page 12.

Configurer le filtrage inter-zones OSPF

Le filtrage des LSA de type 3 de l'ABR étend la capacité d'un ABR qui exécute le protocole OSPF pour filtrer les LSA de type 3 entre les différentes zones OSPF. Une fois qu'une liste de préfixes est configurée, seuls les préfixes spécifiés sont envoyés d'un domaine OSPF à un autre. Tous les autres préfixes sont limités à leur zone OSPF. Vous pouvez appliquer ce type de filtrage de zone au trafic entrant ou sortant d'une zone OSPF, ou au trafic entrant et sortant de cette zone.

Lorsque plusieurs entrées d'une liste de préfixes correspondent à un préfixe donné, l'entrée avec le numéro de séquence le plus faible est utilisée. Par souci d'efficacité, vous pouvez placer les correspondances ou les refus les plus courants près du haut de la liste en leur attribuant manuellement un numéro de séquence inférieur. Par défaut, les numéros de séquence sont générés automatiquement par incréments de 5, en commençant par 5.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **InterArea** > **Add** (ajouter une zone intermédiaire).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer les zones intermédiaires.

Étape 6 Configurez les options de filtrage inter-zones suivantes pour chaque processus OSPF :

- **Processus OSPF** : Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **ID de zone** : la zone pour laquelle les routages doivent être résumés.
- **PrefixList** : le nom du préfixe. Pour ajouter un nouvel objet de liste de préfixes, voir l'étape 5.
- **Sens du trafic** : entrant ou sortant. Choisissez entrant pour filtrer les LSA entrant dans une zone OSPF, ou sortant pour filtrer les LSA sortant d'une zone OSPF. Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.

Étape 7 Cliquez sur **Ajouter** ( ) et saisissez un nom pour la nouvelle liste de préfixes et indiquez si les remplacements doivent être autorisés.

Vous devez configurer une liste de préfixes avant de pouvoir configurer une règle de préfixe.

Étape 8 Cliquez sur **Add** (Ajouter) pour configurer les règles de préfixe, et configurez les paramètres suivants :

- **Action** : sélectionnez **Block** (Bloquer) ou **Allow** (Autoriser) pour l'accès à la redistribution.
- **Sequence No** : Numéro de séquence de routage. Par défaut, les numéros de séquence sont générés automatiquement par incréments de 5, en commençant par 5.
- **IP Address** (adresse IP) : spécifiez le numéro de préfixe au format adresse IP/longueur du masque.
- **Min Prefix Length** : (Facultatif) La longueur minimale du préfixe.
- **Max Prefix Length** : (facultatif) La longueur maximale du préfixe.

Étape 9 Cliquez sur **OK** pour enregistrer la configuration de filtrage inter-zones.

Étape 10 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les règles de filtre OSPF, à la page 13.

Configurer les règles de filtre OSPF

Vous pouvez configurer des filtres LSA ABR de type 3 pour chaque processus OSPF. Les filtres LSA ABR de type 3 permettent uniquement l'envoi de préfixes spécifiés d'une zone à une autre et restreignent tous les autres préfixes. Vous pouvez appliquer ce type de filtrage de zone hors d'une zone OSPF spécifique, dans une zone OSPF spécifique ou à la fois vers et depuis la même zone OSPF. Le filtrage LSA OSPF ABR de type 3 améliore votre contrôle de la distribution des routages entre les zones OSPF.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **Filter Rule** > **Add** (ajouter une règle de filtre) .

Vous pouvez cliquer sur **Edit** ( )ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des règles de filtre.

Étape 6 Configurez les options de règle de filtre suivantes pour chaque processus OSPF :

- **Processus OSPF** : Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **Access List** : liste d'accès pour ce processus OSPF. Pour ajouter un nouvel objet de liste d'accès standard, cliquez sur **Ajouter** ( ) et consultez Configurer les objets ACL standard.

- **Traffic Direction** : Choisissez In ou Out pour la direction du trafic à filtrer. Choisissez In pour filtrer les LSA entrant dans une zone OSPF, ou Out pour filtrer les LSA sortant d'une zone OSPF. Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.
- **Interface** : Interface pour cette règle de filtre.

Étape 7 Cliquez sur **OK** pour enregistrer la configuration de la règle de filtrage.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les adresses de résumé OSPF, à la page 14.

Configurer les adresses de résumé OSPF

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer le périphérique défense contre les menaces pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque de réseau spécifiés. Cette configuration diminue la taille de la base de données d'états de liaison OSPF. Les routes qui correspondent à la paire de masques d'adresses IP spécifiées peuvent être supprimées. La valeur de balise peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Les routes apprises d'autres protocoles de routage peuvent être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Les routages récapitulatifs permettent de réduire la taille de la table de routage.

L'utilisation des routages récapitulatifs pour OSPF amène un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse. Seuls les routages d'autres protocoles de routage qui sont redistribués dans OSPF peuvent être résumés.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **Summary Address** > **Add** (ajouter une adresse résumée) .

Vous pouvez cliquer sur **Edit** ( ) pour modifier ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer les adresses résumées.

Étape 6 Configurez les options d'adresse résumée suivantes pour chaque processus OSPF :

- **Processus OSPF** : Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.

- **Réseau disponible** : l'adresse IP de l'adresse résumée. Sélectionnez un réseau dans la liste des réseaux disponibles et cliquez sur **Add** (Ajouter), ou pour ajouter un nouveau réseau, cliquez sur **Ajouter** (+). Consultez Réseau pour connaître la procédure d'ajout de réseaux.
- **Balise** : valeur décimale de 32 bits associée à chaque routage externe. Cette valeur n'est pas utilisée par OSPF lui-même, mais peut être utilisée pour communiquer des informations entre ASBR.
- **Advertise** (Annonce) : annonce la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

Étape 7 Cliquez sur **OK** pour enregistrer la configuration de l'adresse résumée.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les interfaces et les voisins OSPF, à la page 15.

Configurer les interfaces et les voisins OSPF

Vous pouvez modifier certains paramètres OSPFv2 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello, l'intervalle Dead et la clé d'authentification. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Vous devez définir des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv2 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **Interface** > **Add** (ajouter une interface) .

Vous pouvez cliquer sur **Edit** (✎) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 6 Configurez les options d'interface suivantes pour chaque processus OSPF :

- **Interface** : l'interface que vous configurez.

  Remarque Si le périphérique utilise le routage virtuel, cette liste déroulante affiche uniquement les interfaces qui appartiennent au routeur.

- **Default Cost**(coût par défaut) : le coût d'envoi d'un paquet par l'interface. La valeur par défaut est 10.
- **Priorité** : routeur désigné pour un réseau. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 1. Si vous saisissez 0 pour ce paramètre, le routeur ne pourra pas devenir le routeur désigné ou le routeur de secours désigné.

  Lorsque deux routeurs se connectent à un réseau, tous deux tentent de devenir le routeur désigné. Le périphérique ayant la priorité de routeur la plus élevée devient le routeur désigné. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné. Ce paramètre ne s'applique pas aux interfaces configurées en tant qu'interfaces point à point.
- **Ignorer MTU : OSPF** vérifie si les voisins utilisent la même MTU sur une interface commune. Cette vérification est effectuée lorsque les voisins échangent des paquets DBD. Si la MTU de réception dans le paquet DBD est supérieure à la MTU IP configurée sur l'interface entrante, la contiguïté OSPF n'est pas établie.
- **Filtre de base de données** : utilisez ce paramètre pour filtrer l'interface LSA sortante pendant la synchronisation et l'inondation. Par défaut, OSPF inonde les nouveaux LSA sur toutes les interfaces dans la même zone, sauf l'interface sur laquelle le LSA arrive. Dans une topologie entièrement maillée, cette inondation peut gaspiller de la bande passante et entraîner une utilisation excessive de la liaison et de la CPU. Cocher cette case empêche l'inondation OSPF du LSA sur l'interface sélectionnée.
- **Intervalle Hello** : Spécifie l'intervalle, en secondes, entre les paquets Hello envoyés sur une interface. Les valeurs valides sont comprises entre 1 et 8 192 secondes. La valeur par défaut est 10secondes.

  Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus de trafic est envoyé sur l'interface. Cette valeur doit être la même pour tous les routeurs et serveurs d'accès sur une interface donnée.
- **Délai de transmission** : estimation du temps en secondes pour envoyer un paquet LSA sur l'interface. Les valeurs valides sont comprises entre 1 et 65 535 secondes. La valeur par défaut est de 1 seconde.

  L'âge des LSA dans le paquet de mise à jour est augmenté de la quantité spécifiée par ce champ avant la transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse.
- **Intervalle de retransmission** : temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

  Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles.
- **Intervalle de temps mort** : période en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne. La valeur doit être la même pour tous les nœuds du réseau et peut être comprise entre 1 et 65 535.
- **Multiplicateur Hello** : spécifie le nombre de paquets Hello à envoyer par seconde. Les valeurs valides sont comprises entre 1 et 20.
- **Point à point** : vous permet de transmettre des routes OSPF sur des tunnels VPN.

- **Authentification** : choisissez l'authentification d'interface OSPF parmi les options suivantes :
  - **Aucun** : (par défaut) Désactive l'authentification d'interface.
  - **Authentification de zone** : active l'authentification d'interface à l'aide de MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.
  - **Mot de passe** : fournit un mot de passe en texte clair pour l'authentification par lien virtuel, ce qui n'est pas recommandé lorsque la sécurité est un problème.
  - **MD5** : permet l'authentification MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.

    Remarque Assurez-vous de saisir uniquement des chiffres comme ID de clé MD5.
  - **Chaîne de clé** : permet l'authentification par chaîne de clé. Cliquez sur **Add**(ajouter) et créez la chaîne de clés, puis cliquez sur **Save** (Enregistrer). Pour la procédure détaillée, consultez Création d'objets de chaîne de clé. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie.
- **Saisissez le mot de passe** : le mot de passe que vous configurez si vous choisissez le mot de passe comme type d'authentification.
- **Confirmer le mot de passe** : confirmez le mot de passe que vous avez choisi.

Étape 7 Sélectionnez **Neighbor** > **Add** (ajouter un voisin).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 8 Configurez les paramètres suivants pour chaque processus OSPF :

- **Processus OSPF** : Choisissez 1 ou 2.
- **Neighbor** : choisissez un des voisins dans la liste déroulante ou cliquez sur **Ajouter** ( ) pour ajouter un nouveau voisin. saisissez le nom, la description, le réseau et si vous souhaitez autoriser les remplacements, puis cliquez sur **Save** (Enregistrer).
- **Interface** : choisissez l'interface associée au voisin.

Étape 9 Cliquez sur **OK** pour enregistrer la configuration du voisin.

Étape 10 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Configurer les propriétés avancées OSPF

Les propriétés avancées vous permettent de configurer des options, telles que la génération de messages syslog, les distance de routage administratif, une minuterie LSA et les redémarrages progressifs.

Redémarrages progressifs

Le périphérique défense contre les menaces peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la

restauration des informations du protocole de routage. Cette fonctionnalité est utile lorsqu'une mise à niveau logicielle rapide est planifiée. Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623).

Remarque La capacité NSF est également utile en mode haute disponibilité et mise en grappe.

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Procédure

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

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

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF** > **Advanced (avancé)**.

Étape 5 Sélectionnez **General** (Général) et configurez les éléments suivants :

- **Routeur ID** (ID de routeur) : choisissez Automatic (automatique) ou IP Address (Adresse IP) (apparaît pour les périphériques hors grappe et dans une grappe en mode EtherChannel étendu) ou Cluster Pool (Ensemble de grappes) (apparaît pour une grappe en mode d'interface individuel) comme ID de routeur. Si vous choisissez IP address (adresse IP), saisissez l'adresse IP dans le champ adjacent. Si vous choisissez Cluster Pool, choisissez la valeur de l'ensemble de grappes IPv4 dans le champ déroulant adjacent. Pour en savoir plus sur la création de l'adresse de groupements de grappes, consultez Réserves d'adresses.
- **Ignorer LSA MOSPF** : supprime les messages du journal système lorsque la route reçoit des paquets MOSPF (LSA multicast OSPF) non pris en charge.
- **Compatible RFC 1583** : configure la compatibilité RFC 1583 comme méthode utilisée pour calculer les coûts du récapitulatif de routage. Des boucles de routage peuvent se produire lorsque la compatibilité RFC 1583 est activée. Désactivez-la pour éviter les boucles de routage. La compatibilité RFC doit être définie de manière identique pour tous les routeurs OSPF dans un domaine de routage OSPF.

- **Contiguïté des modifications** : définit les modifications de contiguïté qui entraînent l'envoi des messages syslog.

  Par défaut, un message syslog est généré lorsqu'un voisin OSPF redevient disponible ou tombe en panne. Vous pouvez configurer le routeur pour envoyer un message syslog lorsqu'un voisin OSPF tombe en panne, ainsi qu'un message syslog pour chaque état.

  - **Journaliser les modifications de contiguïté** : permet au périphérique défense contre les menaces d'envoyer un message syslog à chaque fois qu'un voisin OSPF est activé ou désactivé. Ce paramètre est coché par défaut.
  - **Log Adjacency Change Details** (Journaliser les détails sur le changement de contiguïté) : le périphérique défense contre les menaces envoie un message syslog chaque fois qu'un changement d'état se produit, pas seulement quand un voisin monte ou tombe en panne. Ce paramètre est décoché par défaut.

- **Administrative Route Distance** (Distance de routage administrative) : vous permet de modifier les paramètres qui ont été utilisés pour configurer les distances de routage administratives pour les routes IPv6 **externes**, **inter-zones**, **intra-zones** et IPv6. La distance de routage administratif doit être un entier compris entre 1 et 254. La valeur par défaut est 110.
- **LSA Group Pacing** (Rythme de groupe LSA : spécifie l'intervalle en secondes auquel les LSA sont collectés dans un groupe et actualisés, additionnés ou obsolètes. Les valeurs valides vont de 10 à 1 800. La valeur par défaut est 240.
- **Enable Default Information Originate** (activer l'origine des informations par défaut) : cochez la case **Enable** (activer) pour générer une route externe par défaut dans un domaine de routage OSPF et configurer les options suivantes :
  - **Toujours annoncer la route par défaut** : s'assure que la route par défaut est toujours annoncée.
  - **(Metric Value** (Valeur de la métrique) : la métrique utilisée pour générer la voie de routage par défaut. Les valeurs de mesure valides sont comprises entre 0 et 16777214. La valeur par défaut est 10.
  - **Metric Type** (Type de métrique) : le type de lien externe associé à la voie de routage par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides sont 1 (route externe de type 1) et 2 (route externe de type 2). La valeur par défaut est la voie de routage externe de type 2.
  - **RouteMap** (carte de routage) : choisissez le processus de routage qui génère la route par défaut si la carte de routage est satisfaite ou cliquez sur **Ajouter** (+) pour en ajouter une nouvelle. Consultez Configurer une entrée de carte de routage pour ajouter une nouvelle carte de routage.

Étape 6 Cliquez sur **OK** : enregistrez la configuration générale.

Étape 7 Sélectionnez **Non stop Forwarding** (Transfert sans arrêt) et configurez le redémarrage progressif de Cisco NSF pour OSPFv2, pour un périphérique compatible avec NSF ou compatible avec NSF :

Remarque Il existe deux mécanismes de redémarrage progressif pour OSPFv2, Cisco NSF et IETF NSF. Un seul de ces mécanismes de redémarrage progressif peut être configuré à la fois pour une instance OSPF. Un périphérique compatible avec NSF peut être configuré à la fois comme assistant NSF Cisco et comme assistant NSF IETF, mais un périphérique compatible avec NSF peut être configuré en mode Cisco NSF ou IETF NSF à la fois pour une instance OSPF.

a) Cochez la case **Enable Cisco Non Stop Forwarding Capability** (Activer la capacité de transfert sans arrêt de Cisco).
b) (Facultatif) Cochez la case **Cancel NSF restart when non-NSF-aware neighboring networking devices are detected** (Annuler le redémarrage de NSF lorsque des périphériques réseau voisins non sensibles à NSF sont détectés), le cas échéant.
c) (Facultatif) Assurez-vous que la case **Enable Cisco Non Stop Forwarding Helper** (Activer l'aide au transfert sans arrêt de Cisco) est décochée pour désactiver le mode d'assistance sur un périphérique compatible NSF.

Étape 8 Configurez le redémarrage progressif IETF NSF pour OSPFv2, pour un périphérique compatible avec NSF ou compatible avec NSF :

a) Cochez la case **Enable Cisco Non Stop Forwarding Capability** (Activer la capacité de transfert sans arrêt de Cisco).
b) Dans le champ **Longueur de l'intervalle de redémarrage progressif (secondes)**, saisissez l'intervalle de redémarrage en secondes. La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.
c) (Facultatif) Assurez-vous que la case à cocher **Enable IETF non stop forwarding (NSF) for Helper mode** est décochée pour désactiver le mode d'assistance IETF NSF sur un périphérique compatible avec NSF.
d) **Enable Strict Link State advertisement checking** (Activer la vérification stricte de l'annonce de l'état de la liaison) : lorsque cette option est activée, cela indique que le routeur auxiliaire mettra fin au processus de redémarrage du routeur s'il détecte qu'une modification est apportée à un LSA qui serait transmis au routeur qui redémarre, ou si une modification a été effectuée au LSA sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.
e) **Enable IETF Non stop Forwarding** : active le transfert non stop, qui permet au transfert des paquets de données de se poursuivre le long de routes connues pendant que les informations du protocole de routage sont restaurées à la suite d'un basculement. OSPF utilise des extensions du protocole OSPF pour récupérer son état à partir des périphériques OSPF voisins. Pour que la récupération fonctionne, les voisins doivent prendre en charge les extensions de protocole NSF et être prêts à agir en tant qu'« assistants » pour le périphérique qui redémarre. Les voisins doivent également continuer à transférer le trafic de données vers le périphérique qui redémarre pendant que la récupération de l'état du protocole a lieu.

Configurer le protocole OSPFv3

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv3. Pour un périphérique utilisant le routage virtuel, vous pouvez configurer OSPFv3 uniquement pour son routeur virtuel global et non pour son routeur virtuel défini par l'utilisateur.

Configurer les domaines, les résumés de routage et les liens virtuels OSPFv3

Pour activer OSPFv3, vous devez créer un processus de routage OSPFv3, créer une zone pour OSPFv3, activer une interface pour OSPFv3, puis redistribuer le routage dans le processus de routage OSPFv3 ciblé.

Procédure

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

Étape 2 Sélectionnez **Routing** (Routage) > **OSPFv3**.

Étape 3 Par défaut, l'option **Activer le processus 1** est sélectionnée. Vous pouvez activer jusqu'à deux instances de processus OSPF.

Étape 4 Sélectionnez le rôle OSPFv3 dans la liste déroulante et saisissez une description. Les options sont Internal, ABR, ASBR et ABR et ASBR. Consultez À propos d'OSPF, à la page 1 pour obtenir une description des rôles OSPFv3.

Étape 5 Sélectionnez **Area** > **Add** (ajouter une zone intermédiaire).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 6 Sélectionnez **General** et configurez les options suivantes pour chaque processus OSPF :

- **ID de zone** : la zone pour laquelle les routages doivent être résumés.
- **Coût** : la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination. Les valeurs valides sont comprises entre 0 et 16 77 77 2015.
- **Type** : spécifie Normal, NSSA ou Stub. Si vous sélectionnez Normal, il n'y a aucun autre paramètre à configurer. Si vous sélectionnez Stub, vous pouvez choisir d'envoyer des LSA récapitulatifs dans la zone. Si vous sélectionnez NSSA, vous pouvez configurer les trois options suivantes :
  - **Autoriser l'envoi de LSA récapitulatifs dans cette zone** : autorise l'envoi de LSA récapitulatifs dans la zone.
  - **Importe les routes vers les zones normales et NSSA** : permet à la redistribution d'importer les routes vers les zones normales et non vers les zones stubby.
  - **Informations par défaut origine** : génère une route externe par défaut dans un domaine de routage OSPFv3.
- **Mesure** : mesure utilisée pour générer la voie de routage par défaut. La valeur par défaut est 10. Les valeurs de mesure valides sont comprises entre 0 et 16777214.
- **Type de métrique** : le type de métrique est le type de lien externe associé à la voie de routage par défaut annoncée dans le domaine de routage OSPFv3. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.

Étape 7 Cliquez sur **OK** : enregistrez la configuration générale.

Étape 8 (Non applicable au rôle OSPFv3 interne) Sélectionnez **Route Summary** > **Add Route Summary** (Résumé du routage > Ajouter un résumé du routage).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des résumés de routage.

Étape 9 Configurez les options de résumé de routage suivantes pour chaque processus OSPF :

- **Préfixe/longueur IPv6** : préfixe IPv6. Pour ajouter un nouvel objet réseau, cliquez sur **Ajouter** (+). Consultez Réseau pour connaître la procédure d'ajout de réseaux.
- **Coût** : la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination. Les valeurs valides sont comprises entre 0 et 16 77 77 2015.
- **Annoncer** : Annonce la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

Étape 10 Cliquez sur **OK** pour enregistrer la configuration de routage résumée.

Étape 11 (Non applicable au rôle OSPFv3 interne) Sélectionnez **Virtual Link** (lien virtuel), cliquez sur **Add Virtual Link**(ajouter un lien virtuel) et configurez les options suivantes pour chaque processus OSPF :

- **Peer RouterID** : Choisissez l'adresse IP du routeur homologue. Pour ajouter un nouvel objet réseau, cliquez sur **Ajouter** (+). Consultez Réseau pour connaître la procédure d'ajout de réseaux.
- **TTL Security** : active la vérification de sécurité TTL. La valeur du nombre de sauts est un nombre compris entre 1 et 254. La valeur par défaut est 1.

  OSPF envoie des paquets sortants avec une valeur de durée de vie d'en-tête IP (TTL) de 255 et élimine les paquets entrants qui ont des valeurs TTL inférieures à un seuil configurable. Comme chaque périphérique qui transfère un paquet IP décrémente la TTL, les paquets reçus par l'intermédiaire d'une connexion directe (un saut) ont une valeur de 255. Les paquets qui traversent deux sauts ont une valeur de 254, et ainsi de suite. Le seuil de réception est configuré en fonction du nombre maximal de sauts qu'un paquet a pu parcourir.
- **Dead Interval** (intervalle mort) : la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. Cette valeur peut être comprise entre 1 et 65 535.

  L'intervalle mort est un entier non signé. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun.
- **Hello Interval** (intervalle Hello) : le temps en secondes entre les paquets Hello envoyés sur une interface. Cette valeur peut être comprise entre 1 et 65 535. La valeur par défaut est 10.

  L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès sur un réseau spécifique. Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus le trafic acheminé sur l'interface est important.
- **Retransmit Interval** (Intervalle de retransmission) : le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. L'intervalle de retransmission est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 65 535. La valeur par défaut est égale à 5.

  Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles.
- **Transmit Delay** (délai de transmission) : le temps estimée en secondes qui est nécessaire pour envoyer un paquet LSA sur l'interface. La valeur entière doit être supérieure à zéro. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 1.

Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse.

Étape 12 Cliquez sur **OK** pour enregistrer la configuration du lien virtuel.

Étape 13 Cliquez sur **Save** (Enregistrer) sur la page du routeur pour enregistrer vos modifications.

Prochaine étape

Passez à l'étape Configurer la redistribution OSPFv3.

Configurer la redistribution OSPFv3

Le périphérique Cisco Secure Firewall Threat Defense peut contrôler la redistribution des routes entre les processus de routage OSPF. Les règles de redistribution des routages d'un processus de routage vers un processus de routage OSPF sont affichées. Vous pouvez redistribuer les routages détectés par EIGRP, IPS et BGP dans le processus de routage OSPF. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage OSPF.

Procédure

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

Étape 2 Sélectionnez **Routing** (routage) > **OSPF**.

Étape 3 Sélectionnez **Redistribution** et cliquez sur **Add.**

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 4 Configurez les options de redistribution suivantes pour chaque processus OSPF :

- **Protocole source** : le protocole source à partir duquel les routages sont redistribués. Les protocoles pris en charge sont ceux qui sont connectés, OSPF, Static, EIGRP et BGP. Si vous choisissez OSPF, vous devez saisir l'ID de processus dans le champ **Process ID**. Si vous choisissez BGP, vous devez ajouter le numéro de système autonome dans le champ **Numéro** de système autonome.
- **Métrique** : valeur de la métrique pour les routes distribuées. La valeur par défaut est 10. Les valeurs valides sont comprises entre 0 et 16 768214.

  Lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même périphérique, 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.
- **Type de mesure** : Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.

- **Balise** : la balise spécifie la valeur décimale de 32 bits associée à chaque voie de routage externe qui n'est pas utilisée par OSPF lui-même, mais qui peut être utilisée pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides sont comprises entre 0 et 4294967295.
- **Carte de routage** : Vérifie le filtrage de l'importation des routages du protocole de routage source au protocole de routage actuel. Si ce paramètre n'est pas spécifié, toutes les routes sont redistribuées. Si ce paramètre est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée. Vous pouvez aussi ajouter une nouvelle carte de routage en cliquant sur **Ajouter** (+). Consultez Carte de routage pour connaître la procédure d'ajout d'une nouvelle carte de routage.
- **ID de processus** : ID du processus OSPF, 1 ou 2.

  Remarque L'ID de processus est activé, le processus OSPFv3 redistribue une voie de routage apprise par un autre processus OSPFv3.

- **Correspondance** : permet aux routes OSPF d'être redistribuées dans d'autres domaines de routage :
  - **Interne** pour les routages internes à un système autonome spécifique.
  - **Externe 1**pour les routages externes au système autonome, mais importés dans OSPFv3 en tant que routages externes de type 1.
  - **Externe 2** pour les routages externes au système autonome, mais importés dans OSPFv3 en tant que routages externes de type 2.
  - **NSSA externe 1** pour les routages externes au système autonome, mais importés dans OSPFv3 dans une NSSA pour IPv6 en tant que routages externes de type 1.
  - **NSSA externe 2** pour les routages externes au système autonome, mais importés dans OSPFv3 dans une NSSA pour IPv6 en tant que routages externes de type 2.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration de redistribution.

Étape 6 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les préfixes de résumé OSPFv3, à la page 24.

Configurer les préfixes de résumé OSPFv3

Vous pouvez configurer le périphérique défense contre les menaces pour annoncer les routages qui correspondent à une paire de préfixe IPv6 et de masque.

Procédure

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

Étape 2 Sélectionnez **Routing** (Routage) > **OSPFv3**.

Étape 3 Sélectionnez **Summary Prefix** > **Add** (ajouter un préfixe résumé) .

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des préfixes résumés.

Étape 4 Configurez les options de préfixe de résumé suivantes pour chaque processus OSPF :

- **Préfixe/longueur IPv6** : le préfixe IPv6 et l'étiquette de longueur du préfixe. Sélectionnez-en un dans la liste ou cliquez sur **Ajouter** ( ) pour ajouter un nouvel objet réseau. Consultez Réseau pour connaître la procédure d'ajout de réseaux.
- **Annoncer** : annonce les routes qui correspondent à la paire préfixe-masque spécifiée. Décochez cette case pour supprimer les routages qui correspondent à la paire préfixe-masque spécifiée.
- **Balise** (Facultatif) : valeur que vous pouvez utiliser comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration de préfixe résumée.

Étape 6 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les interfaces, l'authentification et les voisins OSPFv3,, à la page 25.

Configurer les interfaces, l'authentification et les voisins OSPFv3,

Vous pouvez modifier certains paramètres OSPFv3 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello et l'intervalle Dead. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Procédure

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

Étape 2 Sélectionnez **Routing** (Routage) > **OSPFv3**.

Étape 3 Sélectionnez **Interface** > **Add** (ajouter une interface) .

Vous pouvez cliquer sur **Edit** (Modifier) pour modifier ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 4 Configurez les options d'interface suivantes pour chaque processus OSPFv3 :

- **Interface** : l'interface que vous configurez.
- **Activer OSPFv3** : Active OSPFv3.
- **Processus OSPF** : Choisissez 1 ou 2.
- **Zone** : ID de zone pour ce processus.

- **Instance** : spécifie l'ID d'instance de zone à affecter à l'interface. Une interface ne peut avoir qu'une seule zone OSPFv3. Vous pouvez utiliser la même zone sur plusieurs interfaces, et chaque interface peut utiliser un ID d'instance de zone différent.

Étape 5 Sélectionnez **Properties** (Propriétés) et configurez les options suivantes pour chaque processus OSPFv3 :

- **Filtrer les publicités d'état de liaison** : filtre les LSA sortants vers une interface OSPFv3. Tous les LSA sortants sont acheminés vers l'interface par défaut.
- **Désactiver la détection de la non-concordance MTU** : désactive la détection de la non-concordance MTU OSPF lors de la réception de paquets DBD. La détection des incompatibilités MTU OSPF est activée par défaut.
- **Réduction de l'inondation** : convertit les LSA normaux en LSA Hors vieillissement, de sorte qu'ils ne soient pas inondés toutes les 3 600 secondes dans l'ensemble des zones.

  Les LSA OSPF sont actualisés toutes les 3 600 secondes. Dans les grands réseaux OSPF, cela peut entraîner une grande quantité de débordements LSA inutiles d'une zone à l'autre.
- **Réseau point à point** : vous permet de transmettre des routes OSPF sur des tunnels VPN. Lorsqu'une interface est configurée comme interface point à point sans diffusion, les restrictions suivantes s'appliquent :
  - Vous ne pouvez définir qu'un seul voisin pour l'interface.
  - Vous devez configurer manuellement le voisin.
  - Vous devez définir une voie de routage statique pointant vers le point terminal de chiffrement.
  - Si OSPF sur un tunnel est exécuté sur l'interface, OSPF standard avec un routeur en amont ne peut pas être exécuté sur la même interface.
  - Vous devez lier la carte de chiffrement à l'interface avant de spécifier le voisin OSPF pour vous assurer que les mises à jour OSPF passent par le tunnel VPN. Si vous liez la carte de chiffrement à l'interface après avoir précisé le voisin OSPF, utilisez la commande **clear local-host all** pour effacer les connexions OSPF afin que les contiguïtés OSPF puissent être établies sur le tunnel VPN.
- **Broadcast** : spécifie que l'interface est une interface de diffusion. Par défaut, cette case est cochée pour les interfaces Ethernet. Décochez cette case pour désigner l'interface comme une interface point à point de non-diffusion. Définir une interface comme point à point, sans diffusion, vous permet de transmettre des routes OSPF sur des tunnels VPN.
- **Coût** : spécifie le coût d'envoi d'un paquet sur l'interface. Les valeurs valides pour ce paramètre sont comprises entre 0 et 255. La valeur par défaut est 1. Si vous saisissez 0 pour ce paramètre, le routeur ne pourra pas devenir le routeur désigné ou le routeur de secours désigné. Ce paramètre ne s'applique pas aux interfaces configurées comme interfaces point à point non de diffusion.

  Lorsque deux routeurs se connectent à un réseau, tous deux tentent de devenir le routeur désigné. Le périphérique ayant la priorité de routeur la plus élevée devient le routeur désigné. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné.
- **Priorité** : pour déterminer le routeur désigné pour un réseau. Les valeurs valides sont comprises entre 0 et 255.
- **Intervalle de temps mort** : période en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne. La valeur doit être la même pour tous les nœuds du réseau et peut varier de 1 à 65 535.

- **Hello Interval** : période de temps en secondes entre les paquets OSPF que le routeur enverra avant que la contiguïté soit établie avec un voisin. Une fois que le périphérique de routage a détecté un voisin actif, l'intervalle du paquet Hello passe de l'heure spécifiée dans l'intervalle d'interrogation à l'heure spécifiée dans l'intervalle Hello. Les valeurs valides vont de 1 à 65535 secondes.
- **Intervalle de retransmission** : temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.
- **Délai de transmission** : estimation du temps en secondes pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration des propriétés.

Étape 7 Sélectionnez **Authentication**(authentification) et configurez les options suivantes pour chaque processus OSPFv3 :

- **Type** : type d'authentification. Les options disponibles sont Zone, Interface et Aucun. L'option Aucun indique qu'aucune authentification n'est utilisée.
- **Indice des paramètres de sécurité** : Numéro de 256 à 4294967295. Configurez ceci si vous avez choisi Interface comme type.
- **Authentification** : type d'algorithme d'authentification. Les valeurs prises en charge sont SHA-1 et MD5. Configurez ceci si vous avez choisi Interface comme type.
- **Clé d'authentification** : lorsque l'authentification MD5 est utilisée, la clé doit comporter 32 chiffres hexadécimaux (16 octets). Lorsque l'authentification SHA-1 est utilisée, la clé doit comporter 40 chiffres hexadécimaux (20 octets).
- **Chiffrer la clé d'authentification** : active le chiffrement de la clé d'authentification.
- **Inclure le chiffrement** : active le chiffrement.
- **Algorithme de chiffrement** : type d'algorithme de chiffrement. La valeur prise en charge est DES. L'entrée NULL indique qu'il n'y a pas de chiffrement. Configurez ceci si vous avez choisi d'**inclure le chiffrement**.
- **Clé de chiffrement** : saisissez la clé de chiffrement. Configurez ceci si vous avez choisi d'**inclure le chiffrement**.
- **Chiffrer la clé** : permet de chiffrer la clé.

Étape 8 Cliquez sur **OK** pour enregistrer la configuration de l'authentification.

Étape 9 Sélectionnez **Neighbor** (voisin), cliquez sur **Add**(ajouter) et configurez les options suivantes pour chaque processus OSPFv3 :

- **Adresse locale du lien** : l'adresse IPv6 du voisin statique.
- **Coût** : active les coûts. Saisissez le coût dans le champ **Coût** et cochez la case **Filtrer les publicités d'état de lien sortants** si vous souhaitez annoncer.
- (Facultatif) **Intervalle d'interrogation** : active l'intervalle d'interrogation. Saisissez le niveau de **priorité** et l' **intervalle d'interrogation** en secondes.

Étape 10 Cliquez sur **Add** (Ajouter) pour ajouter le voisin.

Étape 11 Cliquez sur **OK** pour enregistrer la configuration de l'interface.

Configurer les propriétés avancées OSPFv3

Les propriétés avancées vous permettent de configurer des options, telles que la génération de messages syslog, les distance de routage administratif, le routage OSPFv3 passif, les minuteries LSA et les redémarrages progressifs.

Redémarrages progressifs

Le périphérique défense contre les menaces peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la restauration des informations du protocole de routage. Cette fonctionnalité est utile lorsqu'une mise à niveau logicielle rapide est planifiée. Vous pouvez configurer le redémarrage progressif sur OSPFv3 à l'aide du redémarrage progressif (RFC 5187).

Remarque La capacité NSF est également utile en mode haute disponibilité et mise en grappe.

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Procédure

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

Étape 2 Choisissez **Routage** > **OSPFv3** > **Avancé**.

Étape 3 Dans le champ **Router ID** (ID de routeur), choisissez Automatic (automatique) ou IP Address (adresse IP) (apparaît pour les non-grappes et grappes en mode EtherChannel étendu) ou Groupement de grappes (apparaît pour une grappe en mode d'interface individuel). Si vous choisissez IP Address (adresse IP), saisissez l'adresse IPv6 dans le champ **IP Address** (adresse IP). Si vous choisissez Cluster Pool (Groupement de grappes),

choisissez la valeur du groupement de grappes IPv6 dans le champ **Cluster Pool** . Pour en savoir plus sur la création de l'adresse de groupements de grappes, consultez Réserves d'adresses.

Étape 4 Cochez la case **Ignore LSA MOSPF** (Ignorer LSA MOSPF) si vous souhaitez supprimer les messages du journal système lorsque la route reçoit des paquets OSPF non pris en charge de type 6 (MOSPF).

Étape 5 Sélectionnez **General** (Général) et configurez les éléments suivants :

- **Contiguïté des modifications** : définit les modifications de contiguïté qui entraînent l'envoi des messages syslog.

  Par défaut, un message syslog est généré lorsqu'un voisin OSPF redevient disponible ou tombe en panne. Vous pouvez configurer le routeur pour envoyer un message syslog lorsqu'un voisin OSPF tombe en panne, ainsi qu'un message syslog pour chaque état.

  - **Modifications de contiguïté** : Force le périphérique défense contre les menaces à envoyer un message syslog chaque fois qu'un voisin OSPF redevient disponible ou tombe en panne. Ce paramètre est coché par défaut.
  - **Inclure les détails** : force le périphérique défense contre les menaces à envoyer un message syslog chaque fois qu'un changement d'état se produit, pas seulement quand un voisin redevient disponible ou tombe en panne. Ce paramètre est décoché par défaut.

- **Distance de routage administratif** : vous permet de modifier les paramètres qui ont été utilisés pour configurer les distance de routage administratif pour les routes IPv6 inter-zones, intra-zones et externes. La distance de routage administratif doit être un entier compris entre 1 et 254. La valeur par défaut est 110.
- **Origine des informations par défaut** : Cochez la case **Enable** (activer) pour générer une route externe par défaut dans un domaine de routage OSPFv3 et configurer les options suivantes :
  - **Toujours annoncer** : annoncera toujours la voie de routage par défaut, qu'elle existe ou non.
  - **Mesure** : mesure utilisée pour générer la voie de routage par défaut. Les valeurs de mesure valides sont comprises entre 0 et 16777214. La valeur par défaut est 10.
  - **Metric Type** (Type de métrique) : le type de lien externe associé à la voie de routage par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides sont 1 (route externe de type 1) et 2 (route externe de type 2). La valeur par défaut est la voie de routage externe de type 2.
  - **Carte de routage** : choisissez le processus de routage qui génère la route par défaut si la carte de routage est satisfaite ou cliquez sur **Ajouter** (+) pour en ajouter une nouvelle. Consultez Carte de routage pour ajouter une nouvelle carte de routage.

Étape 6 Cliquez sur **OK** : enregistrez la configuration générale.

Étape 7 Sélectionnez **Passive Interface** (interfaces passives), les interfaces sur lesquelles vous souhaitez activer le routage OSPFv3 passif dans la liste des interfaces disponibles et cliquez sur **Add** (Ajouter) pour les déplacer vers la liste Interfaces sélectionnées.

Le routage passif aide à contrôler l'annonce des informations de routage OSPFv3 et désactive l'envoi et la réception des mises à jour de routage OSPFv3 sur une interface.

Étape 8 Pour enregistrer la configuration de l'interface passive, cliquez sur **Save** (Enregistrer).

Étape 9 Sélectionnez **Timer**(minuteur) et configurez les régulations des LSA et de calcul SPF suivantes :

- **Arrivée** : spécifie le délai minimal en millisecondes qui doit s'écoule entre l'acceptation de la même LSA provenant des voisins. La plage va de 100 à 1 000 millisecondes. La valeur par défaut est de 1 000 millisecondes.
- **Rythme de débordement** : spécifie le temps en millisecondes auquel les LSA de la file d'attente de débordement sont cadencés entre les mises à jour. La plage configurable va de 5 à 100 millisecondes. La valeur par défaut est de 33 millisecondes.
- **Rythme de groupe** : spécifie l'intervalle en secondes auquel les LSA sont rassemblés dans un groupe et rafraîchis, vérifiés ou vieillis. Les valeurs valides vont de 10 à 1 800. La valeur par défaut est 240.
- **Rythme de retransmission** : spécifie le temps en millisecondes auquel les LSA de la file d'attente de retransmission sont régulés. La plage configurable va de 5 à 200 millisecondes. La valeur par défaut est de 66 millisecondes.
- **Limitation de LSA** : spécifie le délai en millisecondes pour générer la première occurrence de LSA. La valeur par défaut est de 0 milliseconde. Le minimum spécifie le délai minimal en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes. La valeur maximale spécifie le délai maximal en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes.

  Remarque Pour la limitation des LSA, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement cette valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

- **Limitation SPF** : spécifie le délai en millisecondes avant de recevoir une modification du calcul SPF. La valeur par défaut est de 5000 millisecondes. La valeur minimale spécifie le délai en millisecondes entre le premier et le deuxième calcul SPF. La valeur par défaut est de 10 000 millisecondes. La valeur maximale spécifie le temps d'attente maximal en millisecondes pour les calculs de SPF. La valeur par défaut est de 10 000 millisecondes.

  Remarque Pour la limitation SPF, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement la valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

Étape 10 Cliquez sur **OK** pour enregistrer la configuration du minuteur LSA.

Étape 11 Sélectionnez **Non stop Forwarding** (Renvoi permanent) et cochez la case **Enable Graceful-Restart Helper** (Activer l'assistant de redémarrage progressif). Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance au redémarrage progressif sur un périphérique compatible avec NSF.

Étape 12 Cochez la case **Enable link state advertisement** (activer l'annonce de l'état des liens) pour activer la vérification stricte des déclarations de l'état des liens.

Lorsqu'elle est cochée, elle indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Étape 13 Cochez la case **Enable graceful-restart (Use when Spanned Cluster or Failover Configured)** (Activer le redémarrage progressif (à utiliser lorsque la grappe étendue ou le basculement sont configurés)) et saisissez l'intervalle de redémarrage progressif en secondes. La valeur est comprise entre 1 et 1 800. La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.

Étape 14 Cliquez sur **OK** pour enregistrer la configuration du redémarrage progressif.

Étape 15 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Historique OSPF

Tableau 1 : Historique des fonctionnalités OSPF

Fonctionnalités	Versions	Défense contre les menaces Minimum	Détails
Prise en charge de BFD pour OSPF v2 et v3	7.4	7.4	Vous pouvez activer BFD sur les interfaces OSPFv2 et OSPFv3. Écrans nouveaux ou modifiés : • **Configuration** > **Installation du périphérique** > **Routage** > **OSPFv2** • **Configuration** > **Installation du périphérique** > **Routage** > **OSPFv3**

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.