Exemple de configuration d'ASA/PIX avec OSPF

Contenu

Introduction

Ce document décrit comment configurer le Cisco ASA pour apprendre les routes par l'intermédiaire de l'Open Shortest Path First (OSPF), exécuter l'authentification, et la redistribution.

Référez-vous à PIX/ASA 8.X : Configurer l'EIGRP sur l'appliance de sécurité adaptable Cisco (ASA) pour plus d'informations sur la configuration EIGRP.

Remarque: Le routage asymétrique n'est pas pris en charge dans ASA/PIX.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Cisco ASA/PIX doit exécuter la version 7.x ou ultérieures.
- L'OSPF n'est pas pris en charge en mode de multi-contexte ; il est pris en charge seulement dans le mode unique.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- L'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) cette exécute la version de logiciel 8.0 et plus tard
- Version de logiciel 6.0 du Cisco Adaptive Security Device Manager (ASDM) et plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Les informations dans ce document s'appliquent également au Pare-feu de la gamme Cisco 500 PIX qui exécute la version de logiciel 8.0 et plus tard.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

L'OSPF emploie un algorithme d'état de lien afin de construire et calculer le plus court chemin à toutes les destinations connues. Chaque routeur dans une zone OSPF contient une base de données identique d'état de lien, qui est une liste de chacun des interfaces utilisables de routeur et des voisins accessibles.

Les avantages de l'OSPF au-dessus du RIP incluent :

- Des mises à jour de base de données d'état de lien OSPF envoyées à moins fréquemment que DÉCHIRENT des mises à jour, et la base de données d'état de lien sont est mise à jour immédiatement plutôt que graduellement pendant que les informations périmées sont chronométrées.
- Conduisant des décisions sont basés sur le coût, qui est une indication du temps système exigé pour envoyer des paquets à travers une certaine interface. Les dispositifs de sécurité calculent le coût d'une interface basée sur la bande passante de lien plutôt que le nombre de sauts à la destination. Le coût peut être configuré pour spécifier des chemins préférentiels.

L'inconvénient des shortests path first algorithm est qu'ils exigent beaucoup de cycles CPU et mémoire.

Les dispositifs de sécurité peuvent exécuter deux processus de protocole OSPF simultanément, sur différents ensembles d'interfaces. Vous pourriez vouloir exécuter deux processus si vous avez

des interfaces qui utilisent les mêmes adresses IP (NAT permet à ces interfaces pour coexister, mais l'OSPF ne permet pas des adresses superposantes). Ou vous pourriez vouloir exécuter un processus sur l'intérieur, et des autres sur l'extérieur, et redistribuez un sous-ensemble d'artères entre les deux processus. De même, vous pourriez devoir isoler des adresses privées des annonces publiques.

Vous pouvez redistribuer des artères dans un processus de routage OSPF d'un autre processus de routage OSPF, un processus de routage de RIP, ou de la charge statique et des routes connectées configurées sur les interfaces OSPF-activées.

Les dispositifs de sécurité prennent en charge ces caractéristiques OSPF :

- Support d'intra-zone, d'interarea, et d'externe (artères de type I et de type II).
- Support d'une liaison virtuelle.
- Inondation LSA OSPF.
- Authentification aux paquets OSPF (mot de passe et authentification de MD5).
- Soutien de configurer les dispositifs de sécurité en tant qu'un routeur indiqué ou routeur de sauvegarde indiqué. Les dispositifs de sécurité peuvent également être installés comme ABR. Cependant, la capacité de configurer les dispositifs de sécurité comme ASBR est limitée aux informations par défaut seulement (par exemple, injectant un default route).
- Soutien des zones d'extrémité et des non-ainsi-tronqué-zones.
- Filtrage LSA du routeur type-3 de borne de zone.

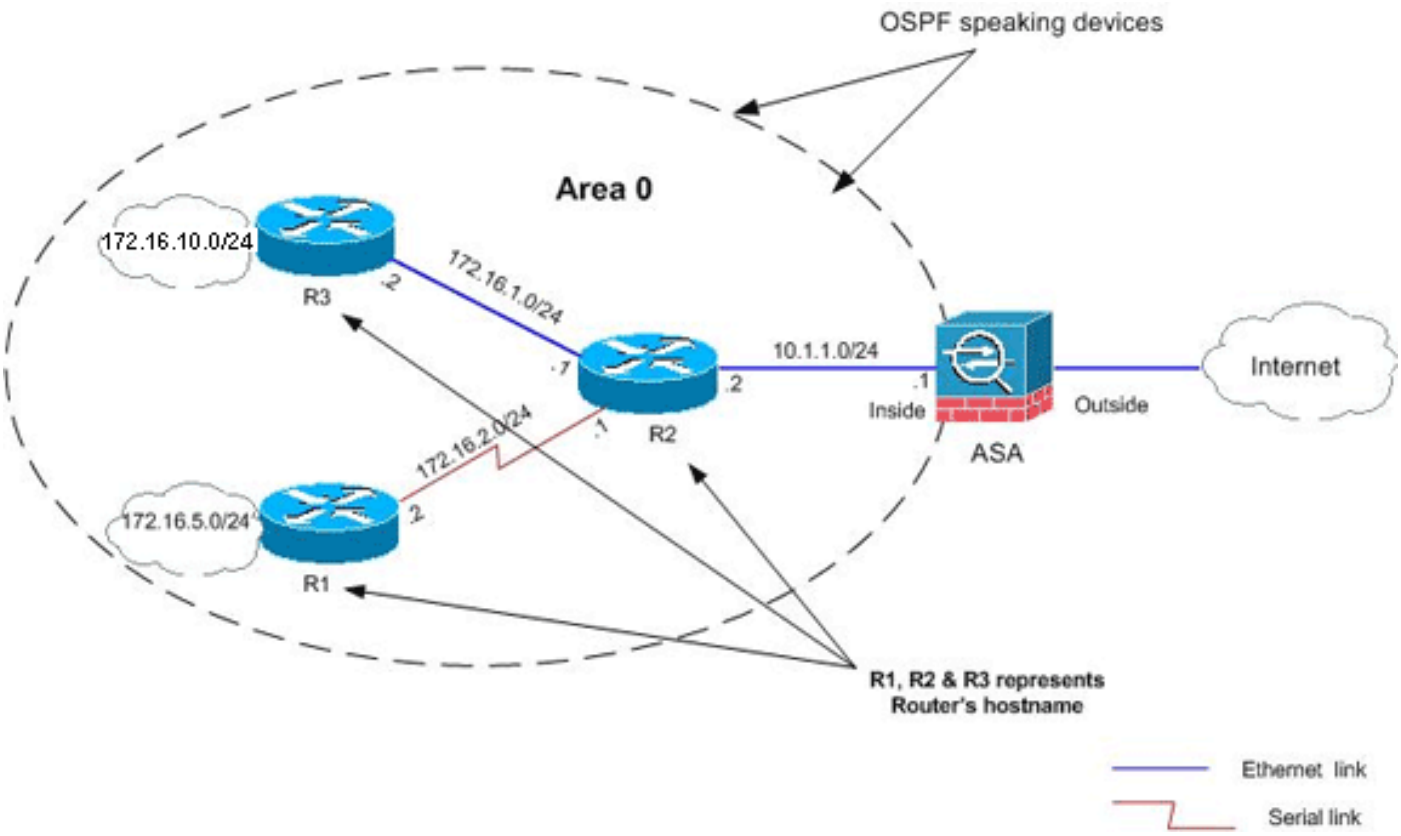
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



En cette topologie du réseau, l'adresse IP d'interface interne de Cisco ASA est 10.1.1.1/24. Le but est de configurer l'OSPF sur Cisco ASA afin d'apprendre des artères aux réseaux internes (172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 et 172.16.10.0/24) dynamiquement par le routeur contigu (R2). R2 apprend les artères aux réseaux internes distants par les deux autres Routeurs (R1 et R3).

Configurations

Ce document utilise les configurations suivantes :

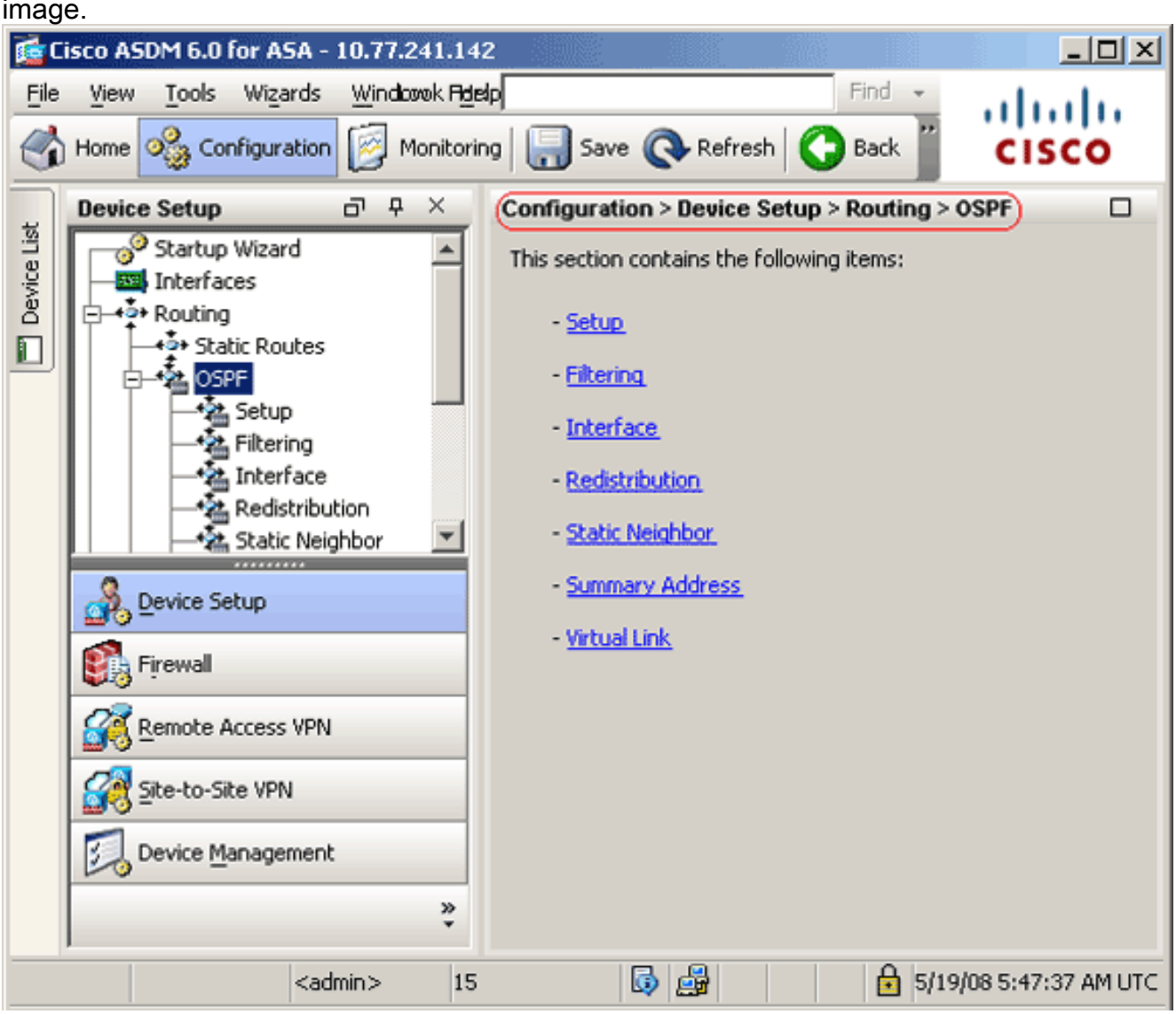
- Configuration ASDM
- Configurez l'authentification OSPF
- Configuration de Cisco ASA CLI
- Configuration CLI du routeur Cisco IOS (R2)
- Configuration CLI du routeur Cisco IOS (R1)
- Configuration CLI du routeur Cisco IOS (R3)
- Redistribuez dans l'OSPF avec l'ASA

Configuration ASDM

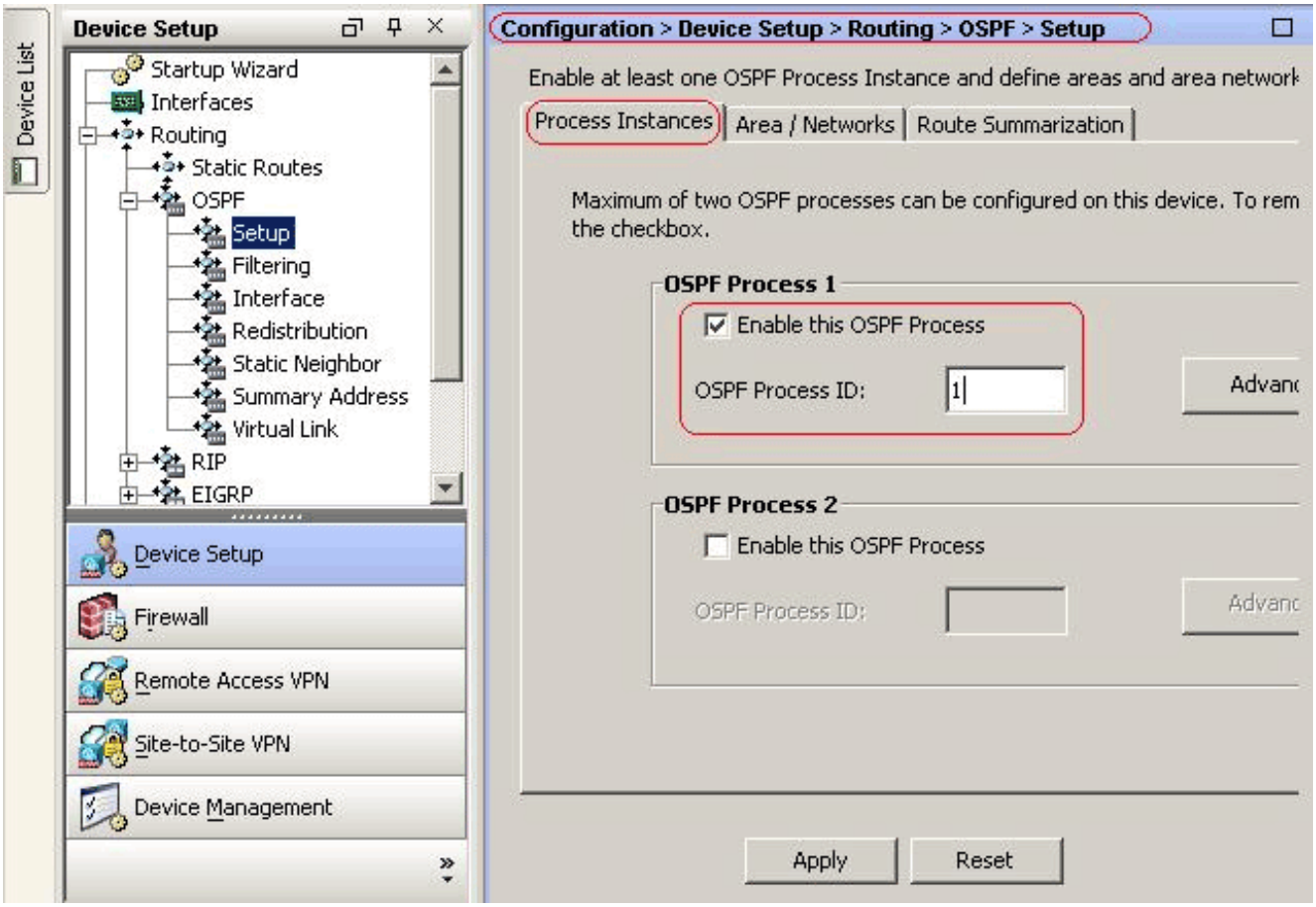
Adaptive Security Device Manager (ASDM) est une application navigateur utilisée pour configurer et surveiller le logiciel sur des dispositifs de sécurité. L'ASDM est chargé des dispositifs de sécurité, et puis utilisé pour configurer, surveiller, et gérer le périphérique. Vous pouvez également utiliser le lanceur ASDM (Windows seulement) afin de lancer l'application ASDM plus rapide que l'applet Java. Cette section décrit les informations que vous devez configurer les caractéristiques décrites dans ce document avec l'ASDM.

Terminez-vous ces étapes afin de configurer l'OSPF à Cisco ASA :

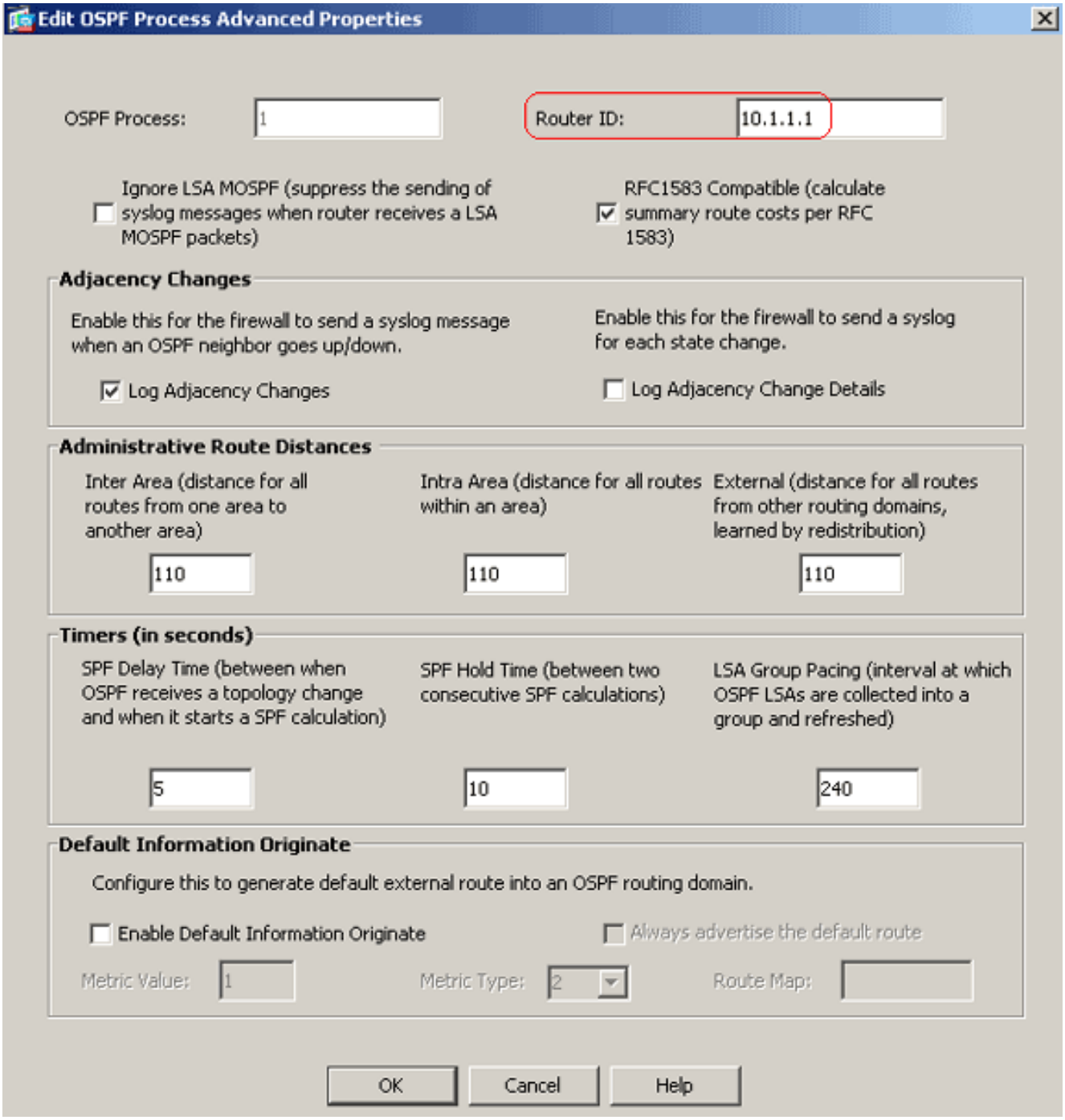
1. Procédure de connexion à Cisco ASA avec l'ASDM.
2. Naviguez vers la **configuration > l'installation de périphérique > le routage > la** zone **OSPF de l'**interface ASDM, suivant les indications de cette image.



3. Activez le processus de routage OSPF sur l'onglet d'**exemples d'installation > de processus**, suivant les indications de cette image. Dans cet exemple, le processus d'ID OSPF est **1.**



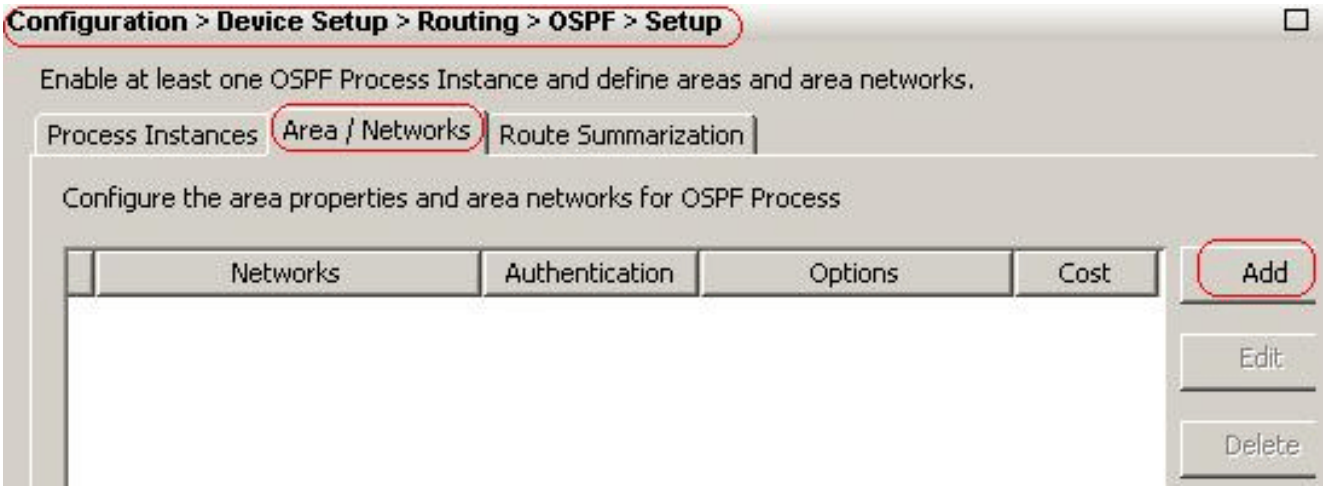
4. Vous pouvez cliquer sur **avancé** sur l'onglet d'**exemples d'installation > de processus** afin de configurer des paramètres de processus avancés facultatifs de routage OSPF. Vous pouvez éditer des configurations de processus-particularité, telles que l'ID de routeur, des modifications de contiguïté, des distances administratives d'artère, des temporisateurs, et les informations par défaut lancent des configurations.



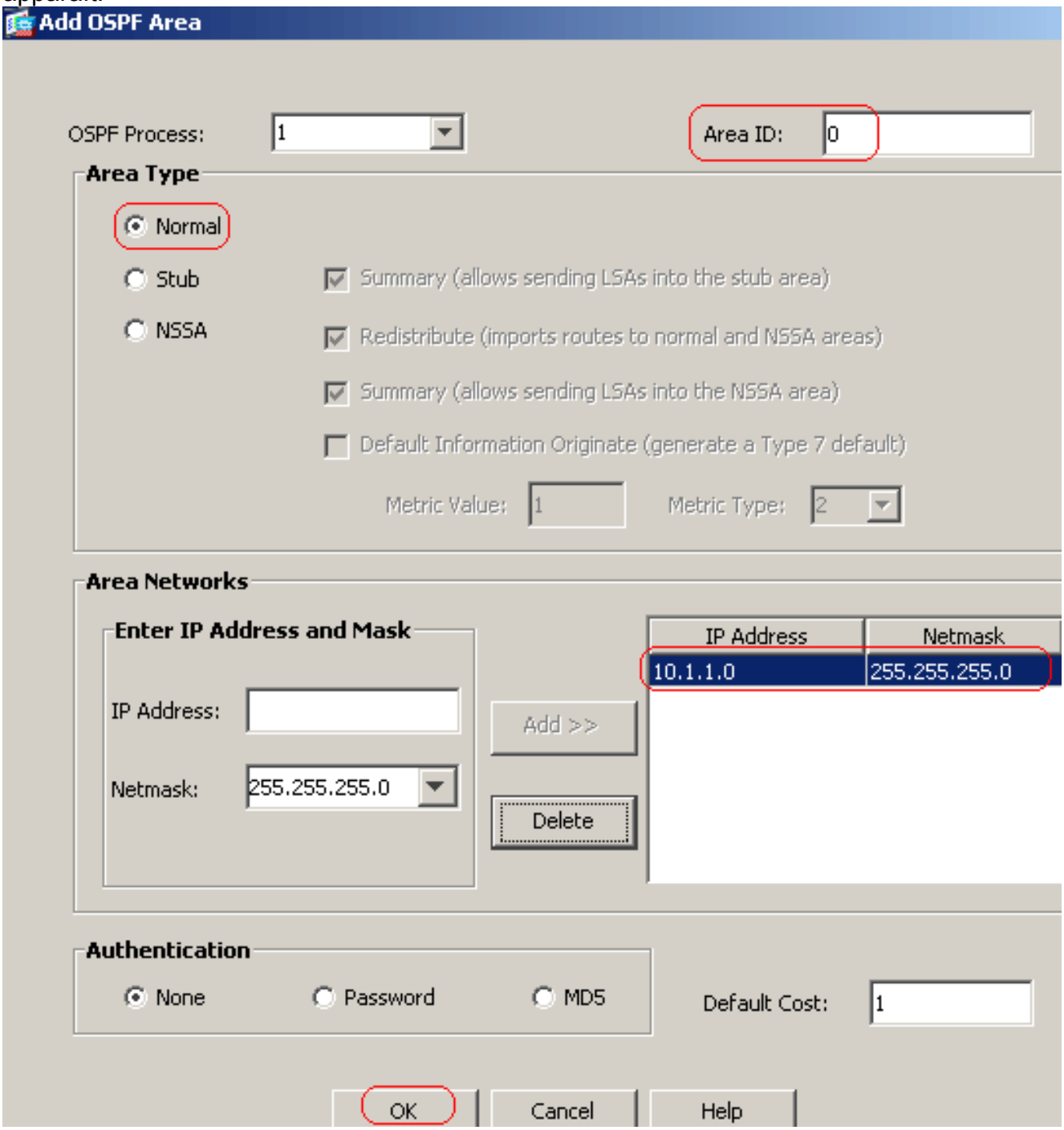
Cette liste décrit chaque champ :Processus OSPF — Affiche le processus OSPF que vous configurez. Vous ne pouvez pas changer cette valeur.ID de routeur — Afin d'utiliser un ID de routeur fixe, écrivez un ID de routeur dans le format d'adresse IP dans le domaine d'ID de routeur. Si vous laissez ce blanc de valeur, l'adresse IP de plus haut niveau sur les dispositifs de sécurité est utilisée comme ID de routeur.Dans cet exemple, l'ID de routeur est statiquement configuré avec l'adresse IP de l'interface interne (10.1.1.1).Ignore lsa mospf — Cochez cette case afin de supprimer l'envoi des messages du journal système quand les dispositifs de sécurité reçoivent des paquets LSA du type 6 (MOSPF). Cette configuration est décochée par défaut.RFC 1583 compatible — Cochez cette case afin de calculer des coûts de route récapitulative par RFC 1583. Décochez cette case afin de calculer des coûts de route récapitulative par RFC 2328. Afin de réduire la possibilité des boucles de routage, tous les périphériques OSPF dans un routing domain OSPF devraient avoir la compatibilité RFC réglée identiquement. Cette configuration est sélectionnée par défaut.Modifications de contiguïté — Contient les configurations qui définissent les modifications de contiguïté qui causent des messages du journal système d'être envoyés.Modifications de contiguïté de log

— Cochez cette case afin de faire envoyer les dispositifs de sécurité un message du journal système toutes les fois qu'un voisin OSPF va en haut ou en bas. Cette configuration est sélectionnée par défaut.La contiguïté de log change le détail — Cochez cette case afin de faire envoyer les dispositifs de sécurité un message du journal système toutes les fois que n'importe quelle modification d'état se produit, pas au moment même où un voisin va en haut ou en bas. Cette configuration est décochée par défaut.Distances administratives d'artère — Contient les configurations pour les distances administratives des artères basées sur le type d'artère.Zone inter — Place la distance administrative pour toutes les artères d'une zone à l'autre. Chaîne de valeurs valides de 1 à 255. La valeur par défaut est 100.Intra zone — Place la distance administrative pour toutes les artères dans une zone. Chaîne de valeurs valides de 1 à 255. La valeur par défaut est 100.Externe — Place la distance administrative pour toutes les artères d'autres domaines de routage qui sont appris par la redistribution. Chaîne de valeurs valides de 1 à 255. La valeur par défaut est 100.Temporisateurs — Contient les configurations utilisées pour configurer des temporisateurs de arpenter LSA et de calcul SPF.Temps de retard SPF — Spécifie le temps entre quand l'OSPF reçoit une modification de topologie et quand les débuts de calcul SPF. Chaîne de valeurs valides de 0 à 65535. La valeur par défaut est 5.Durée d'attente SPF — Spécifie la durée d'attente entre les calculs consécutifs SPF. Chaîne de valeurs valides de 1 à 65534. La valeur par défaut est 10.Arpenter de groupe LSA — Spécifie l'intervalle auquel LSAs sont collectés dans un groupe et régénérés, checksummed, ou vieillis. Chaîne de valeurs valides de 10 à 1800. La valeur par défaut est 240.Les informations par défaut commencent — Contient les configurations utilisées par un ASBR pour générer une artère externe par défaut dans un routing domain OSPF.Les informations par défaut d'enable commencent — Cochez cette case afin d'activer la génération du default route dans le routing domain OSPF.Annoncez toujours le default route — Cochez cette case afin d'annoncer toujours le default route. Cette option est décochée par défaut.Valeur métrique — Spécifie la mesure d'OSPF par défaut. Chaîne de valeurs valides de 0 à 16777214. La valeur par défaut est 1.Type métrique — Spécifie le type de liaison externe associé avec le default route annoncé dans le routing domain OSPF. Les valeurs valides sont 1 ou 2, indiquant un type 1 ou une artère externe de type-2. La valeur par défaut est 2.Mappage de route — (*facultatif*) le nom du mappage de route à appliquer. Le processus de routage génère le default route si le mappage de route est satisfait.

5. Après que vous vous terminiez les étapes précédentes, définissez les réseaux et les interfaces qui participent au routage OSPF sur l'onglet d'**installation > de zone/réseaux**, et puis cliquez sur Add suivant les indications de cette image
:



La boîte de dialogue de zone OSPF d'ajouter apparaît.

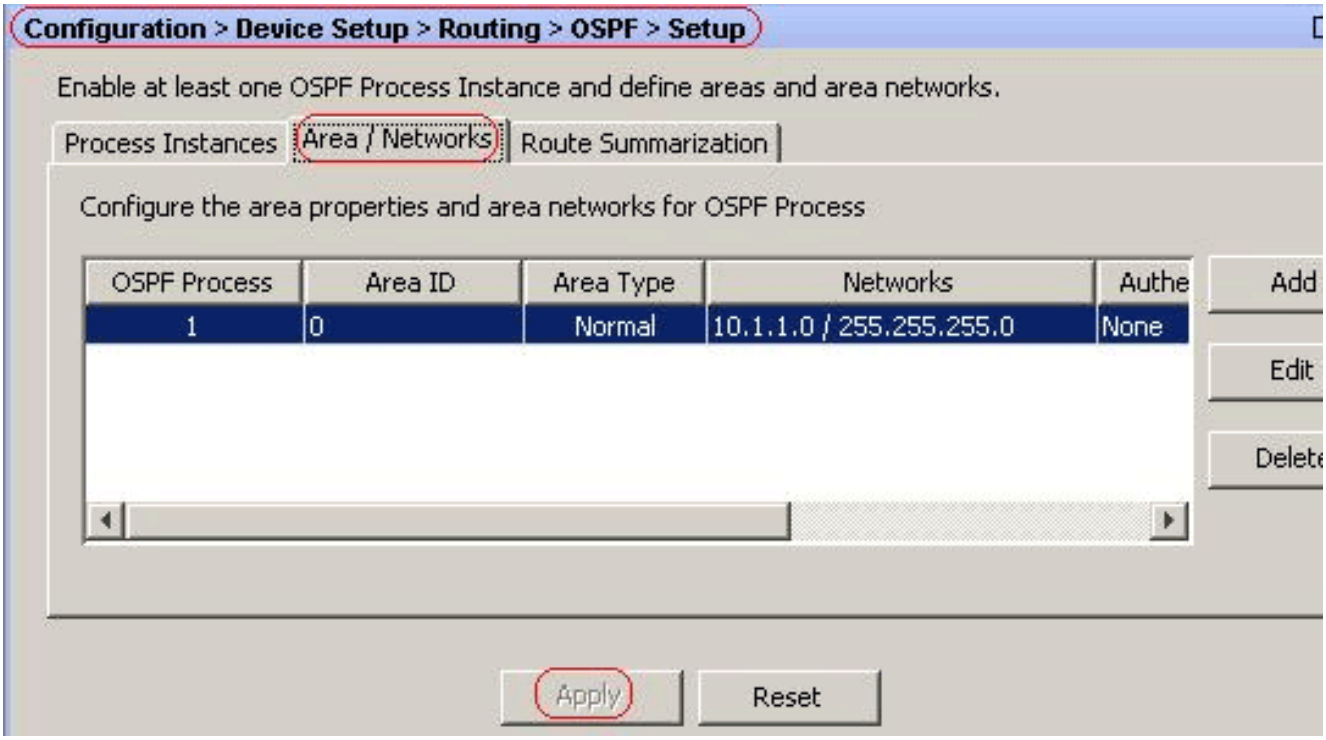


Dans cet exemple, le seul réseau qui est ajouté est le réseau intérieur (10.1.1.0/24) puisque l'OSPF est activé seulement sur l'interface interne.**Remarque:** Se connecte par interface seulement à une adresse IP qui font partie des réseaux définis participent au processus de routage OSPF.

6. Cliquez sur **OK**.Cette liste décrit chacune met en place :Processus OSPF — Quand vous ajoutez une nouvelle zone, choisissez l'ID pour le processus OSPF. S'il y a seulement un processus OSPF activé sur les dispositifs de sécurité, alors ce processus est sélectionné par défaut. Quand vous éditez une zone existante, vous ne pouvez pas changer l'ID de processus OSPF.ID de zone — Quand vous ajoutez une nouvelle zone, écrivez l'ID de zone. Vous pouvez spécifier l'ID de zone comme nombre décimal ou adresse IP. Les valeurs décimales valides s'étendent de 0 à 4294967295. Vous ne pouvez pas changer l'ID de zone quand vous éditez une zone existante.Dans cet exemple, l'ID de zone est **0**.Type de zone — Contient les configurations pour le type de zone étant configuré.Normal — Choisissez cette

option afin de faire à la zone par zone standard OSPF. Cette option est sélectionnée par défaut quand vous créez d'abord une zone.Stub — Choisissez cette option afin de faire à la zone par zone d'extrémité. Les zones d'extrémité n'ont aucuns Routeurs ou zone au delà de lui. Les zones d'extrémité empêchent EN TANT QUE LSAs externe (type 5 LSAs) de l'inondation dans la zone d'extrémité. Quand vous créez une zone d'extrémité, vous pouvez décocher la case récapitulative pour empêcher les LSA récapitulatifs (type 3 et 4) de l'inondation dans la zone.Résumé — Quand la zone étant définie est une zone d'extrémité, décochez cette case afin d'empêcher LSAs d'être envoyé dans la zone d'extrémité. Cette case est sélectionnée par défaut pour des zones d'extrémité.NSSA — Choisissez cette option afin de faire à la zone par zone non-ainsi-tronquée. NSSAs reçoivent le type 7 LSAs. Quand vous créez un NSSA, vous pouvez décocher la case récapitulative afin d'empêcher des LSA récapitulatifs d'être inondée dans la zone. En outre, vous pouvez décocher la case de redistribuer et les informations de Defautl d'enable commencent afin de désactiver la redistribution de routage.Redistribuez — Décochez cette case afin d'empêcher des artères d'être importé dans le NSSA. Cette case est sélectionnée par défaut.Résumé — Quand la zone étant définie est un NSSA, décochez cette case afin d'empêcher LSAs d'être envoyé dans la zone d'extrémité. Cette case est sélectionnée par défaut pour NSSAs.Les informations par défaut commencent — Cochez cette case afin de générer un par défaut du type 7 dans le NSSA. Cette case est décochée par défaut.Valeur métrique — Écrivez une valeur afin de spécifier la valeur métrique OSPF pour le default route. Chaîne de valeurs valides de 0 à 16777214. La valeur par défaut est 1.Type métrique — Choisissez une valeur afin de spécifier le type métrique OSPF pour le default route. Les choix sont 1 (type 1) ou 2 (type-2). La valeur par défaut est 2.Réseaux de zone — Contient les configurations qui définissent une zone OSPF.Écrivez l'adresse IP et la masquez — Contient les configurations utilisées pour définir les réseaux dans la zone.Adresse IP — Écrivez l'adresse IP du réseau ou la hébergez pour être ajoutée à la zone. Employez 0.0.0.0 avec un netmask de 0.0.0.0 pour créer la zone par défaut. Vous pouvez utiliser 0.0.0.0 dans seulement une zone.Netmask — Choisissez le masque de réseau pour l'adresse IP ou le hébergez pour être ajouté à la zone. Si vous ajoutez un hôte, choisissez le masque de 255.255.255.255.Dans cet exemple, **10.1.1.0/24** est le réseau à configurer.Ajoutez — Ajoute le réseau défini dans la région d'adresse IP et de masque d'entrer à la zone. Le réseau ajouté apparaît dans la table réseau de zone.Effacement — Supprime le réseau sélectionné de la table réseau de zone.Réseaux de zone — Affiche les réseaux définis pour la zone.Adresse IP — Affiche l'adresse IP du réseau.Netmask — Affiche le masque de réseau pour le réseau.Authentification — Contient les configurations pour l'area authentication OSPF.Aucun — Choisissez cette option afin de désactiver l'area authentication OSPF. C'est la valeur par défaut.Mot de passe — Choisissez cette option afin d'utiliser un mot de passe des textes clairs pour l'area authentication. Cette option n'est pas recommandée où la Sécurité est un souci.MD5 — Choisissez cette option afin d'utiliser l'authentification de MD5.Coût par défaut — Spécifiez un coût par défaut pour la zone. Chaîne de valeurs valides de 0 à 65535. La valeur par défaut est 1.

7. Cliquez sur
   Apply.



8. Sur option, vous pouvez définir des filtres d'artère sur le volet de règles de filtrage. Le filtrage d'artère fournit plus de contrôle des artères qui sont permises pour être envoyées ou reçues dans les mises à jour OSPF.
9. Vous pouvez sur option configurer la redistribution de routage. Cisco ASA peut redistribuer des artères découvertes par le RIP et l'EIGRP dans le processus de routage OSPF. Vous pouvez également redistribuer la charge statique et les routes connectées dans le processus de routage OSPF. Définissez la redistribution de routage sur le volet de redistribution.
10. Des paquets HELLO OSPF sont envoyés comme paquets de multidiffusion. Si un voisin OSPF se trouve à travers un réseau de nonbroadcast, vous devez manuellement définir ce voisin. Quand vous définissez manuellement un voisin OSPF, bonjour des paquets sont envoyés à ce voisin comme messages d'unicast. Afin de définir les voisins statiques OSPF, allez au volet voisin statique.
11. Des artères apprises d'autres protocoles de routage peuvent être récapitulées. La mesure utilisée pour annoncer le résumé est la plus petite mesure des artères plus spécifiques. Les routes récapitulatives aident à réduire la taille de la table de routage.Utilisant des routes récapitulatives pour l'OSPF fait annoncer un OSPF ASBR une artère externe car un agrégat pour toutes les artères redistribuées qui sont couvertes par l'adresse. Seulement des artères d'autres protocoles de routage qui sont redistribués dans l'OSPF peuvent être récapitulées.
12. Dans le volet de liaison virtuelle, vous pouvez ajouter une zone à un réseau OSPF, et il n'est pas possible de connecter la zone directement à la zone fédératrice ; vous devez créer une liaison virtuelle. Une liaison virtuelle connecte deux périphériques OSPF qui ont un espace commun, appelés la zone de transit. Un des périphériques OSPF doit être connecté à la zone fédératrice.

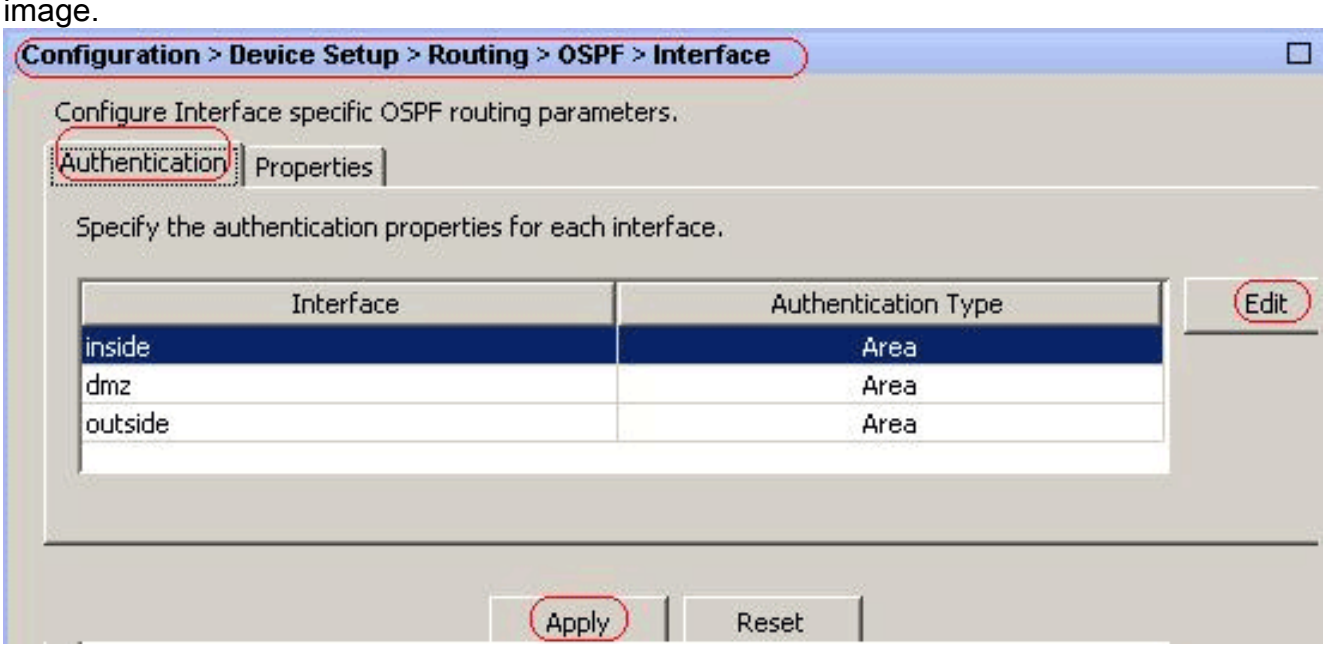
Configurez l'authentification OSPF

Cisco ASA prend en charge l'authentification de MD5 des mises à jour de routage du protocole de routage OSPF. Le condensé introduit par MD5 en chaque paquet OSPF empêche l'introduction des messages non autorisés ou faux de routage des sources inapprouvées. L'ajout de l'authentification à vos messages OSPF s'assure que vos Routeurs et Cisco ASA reçoivent

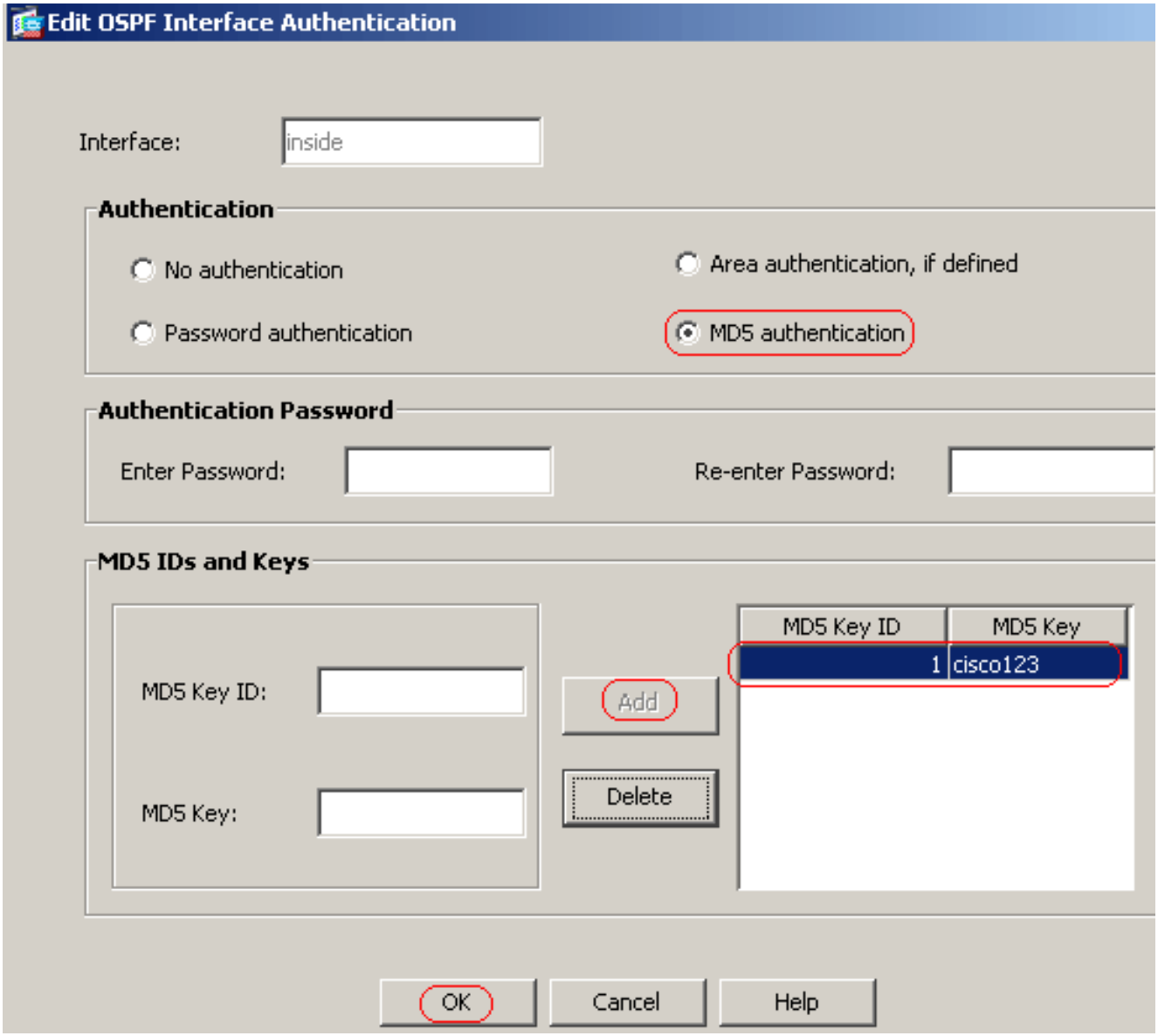
seulement des messages de routage d'autres périphériques de routage qui sont configurés avec la même clé pré-partagée. Sans cette authentification configurée, si quelqu'un introduit un autre périphérique de routage avec les informations différentes ou contraires d'artère sur le réseau, les tables de routage sur vos Routeurs ou Cisco ASA peuvent devenir corrompues, et une attaque par déni de service peut s'ensuivre. Quand vous ajoutez l'authentification aux messages EIGRP envoyés entre vos périphériques de routage (qui inclut l'ASA), elle empêche l'ajout utile ou accidentel d'un autre routeur au réseau et à n'importe quel problème.

L'authentification d'artère OSPF est par interface configuré. Tous les voisins OSPF sur des interfaces configurées pour l'authentification de message OSPF doivent être configurés avec la mêmes authentication mode et clé pour que des contiguïtés soient établies.

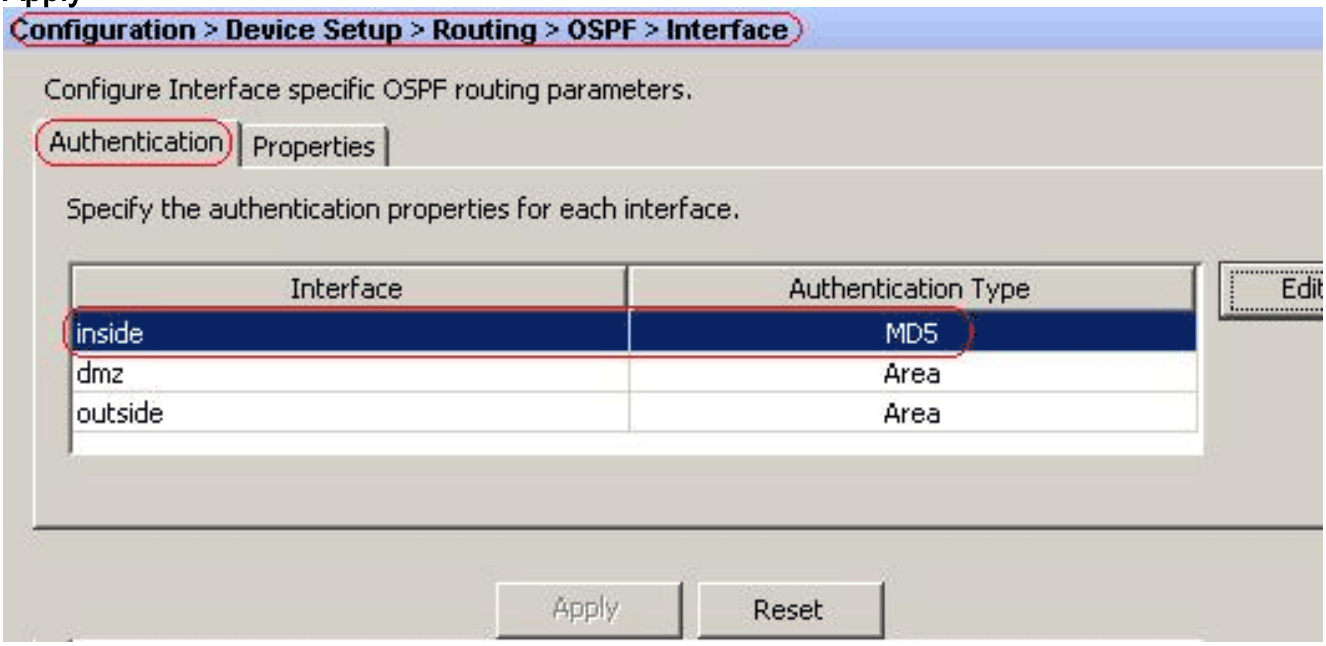
Terminez-vous ces étapes afin d'activer l'authentification de MD5 OSPF sur Cisco ASA :

1. Sur l'ASDM, naviguez vers la **configuration > l'installation de périphérique > le routage > l'OSPF > l'interface**, et puis cliquez sur l'onglet d'**authentification** suivant les indications de cette
   image.
   

   Dans ce cas, l'OSPF est activé sur l'interface interne.
2. Choisissez l'**interface interne**, et cliquez sur Edit.
3. Sous l'authentification, choisissez l'**authentification de MD5**, et ajoutez plus d'informations sur des paramètres d'authentification ici.Dans ce cas, la clé pré-partagée est **cisco123**, et l'ID de clé est
   1.



4. Cliquez sur **OK**, puis sur **Apply**.



Configuration de Cisco ASA CLI

Cisco ASA

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names !--- Inside interface
configuration interface Ethernet0/1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0
ospf cost 10 !--- OSPF authentication is configured on
the inside interface ospf message-digest-key 1 md5
<removed> ospf authentication message-digest ! !---
Outside interface configuration interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ospf cost 10 ! !--- Output Suppressed icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-602.bin no asdm history enable arp timeout
14400 ! !--- OSPF Configuration router ospf 1 network
10.1.1.0 255.255.255.0 area 0 log-adj-changes ! !---
This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

Configuration CLI du routeur Cisco IOS (R2)

Routeur Cisco IOS (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0 ip address 10.1.1.2 255.255.255.0 ip ospf
authentication message-digest ip ospf message-digest-key
1 md5 cisco123 !--- Output Suppressed !--- OSPF
Configuration router ospf 1 log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0 network 172.16.1.0
0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0
```

Configuration CLI du routeur Cisco IOS (R1)

Routeur Cisco IOS (R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1 log-adjacency-changes network 172.16.5.0
0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0
```

Configuration CLI du routeur Cisco IOS (R3)

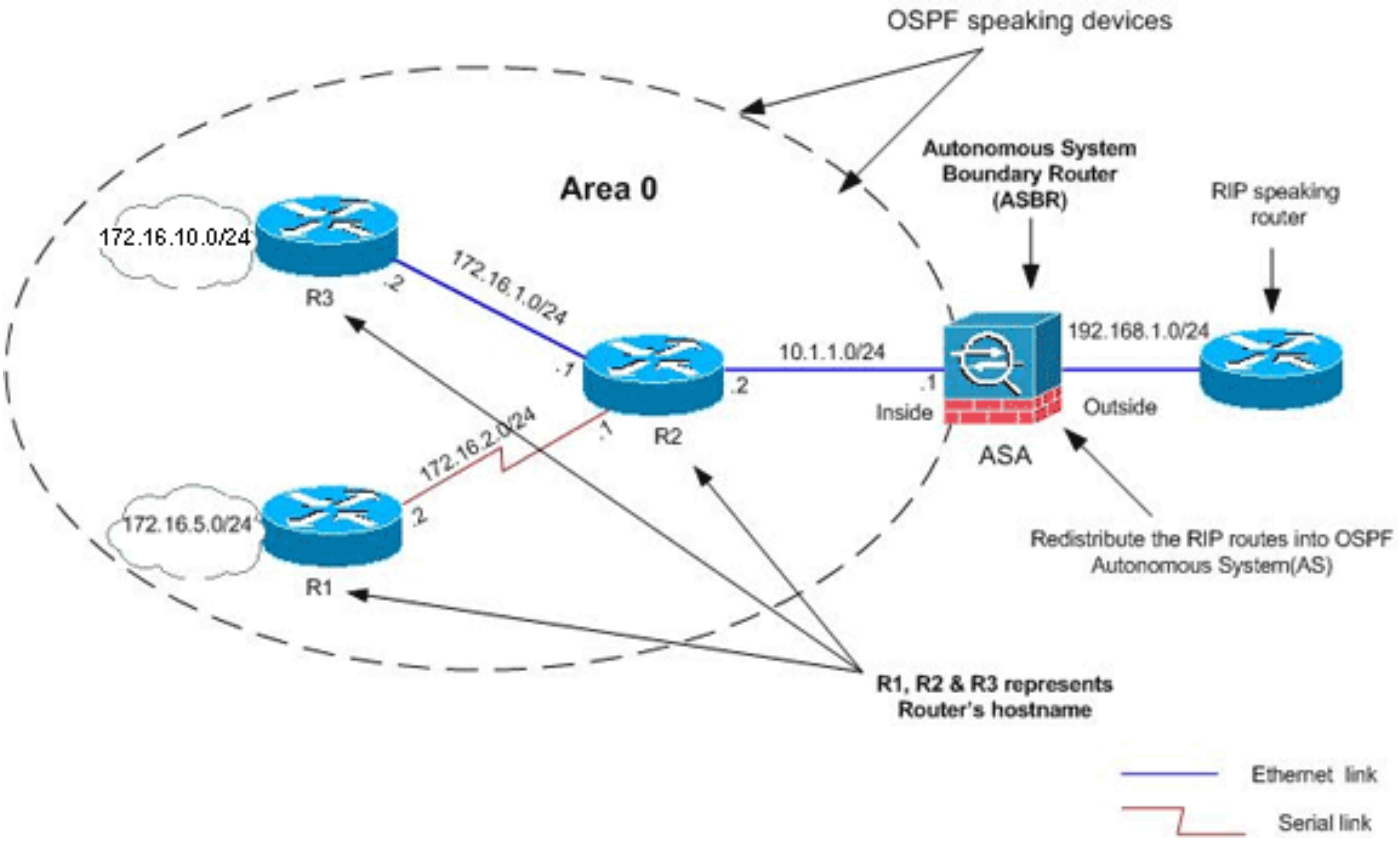
Routeur Cisco IOS (R3)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1 log-adjacency-changes network 172.16.1.0
0.0.0.255 area 0 network 172.16.10.0 0.0.0.255 area 0
```

Redistribuez dans l'OSPF avec l'ASA

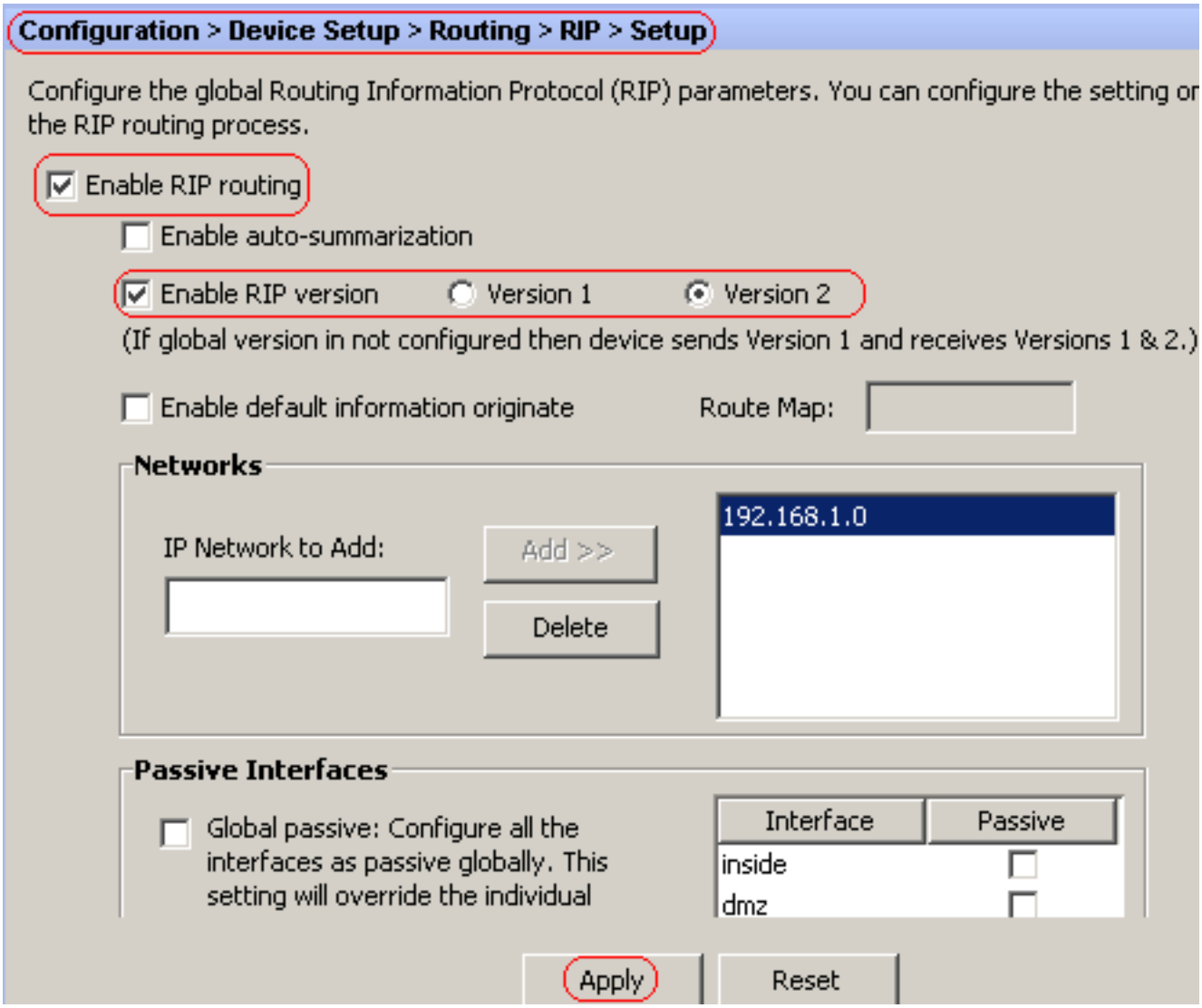
Comme cité précédemment, vous pouvez redistribuer des artères dans un processus de routage OSPF d'un autre processus de routage OSPF, un processus de routage de RIP, ou de la charge statique et des routes connectées configurées sur les interfaces OSPF-activées.

Dans cet exemple, redistribuant les routes RIP dans l'OSPF avec le schéma de réseau comme affiché :

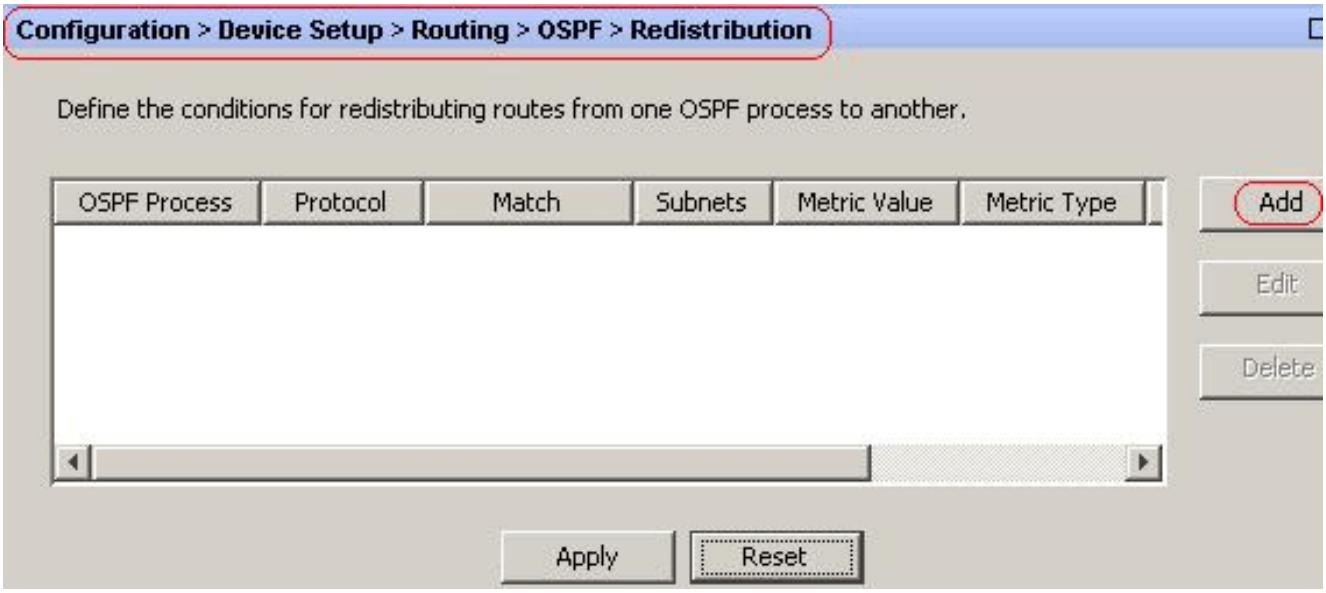


Configuration ASDM

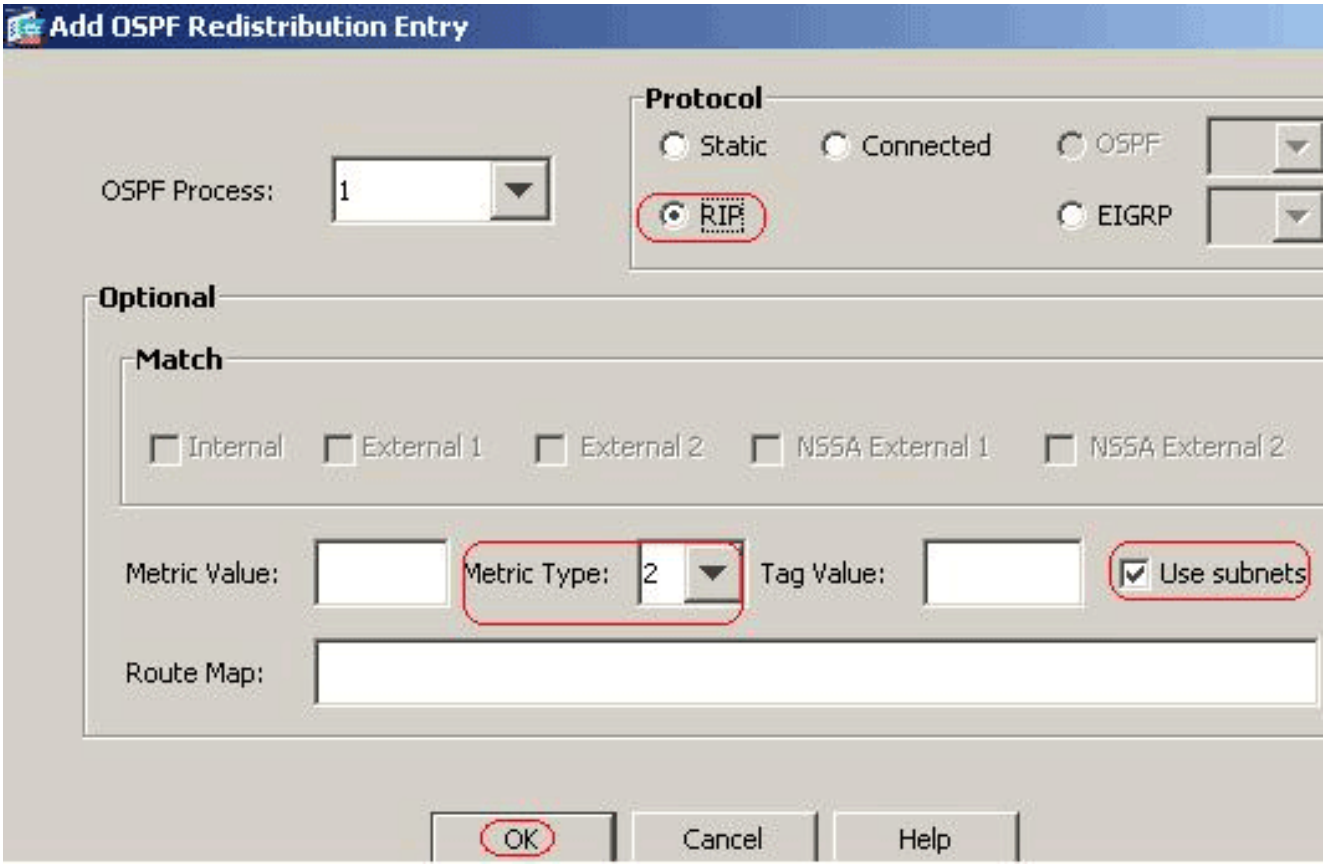
1. Choisissez la **configuration > l'installation de périphérique > le routage > le RIP > installé** afin d'activer le RIP, et ajoutez le réseau 192.168.1.0 suivant les indications de cette image.



2. Cliquez sur **Apply**.
3. Choisissez la **configuration > l'installation de périphérique > le routage > l'OSPF > la redistribution > ajoutent** afin de redistribuer des routes RIP dans l'OSPF.



4. Cliquez sur **OK**, puis sur **Apply**.



Configuration équivalente CLI

La configuration CLI de l'ASA pour redistribuent le RIP dans l'OSPF AS
router ospf 1 network 10.1.1.0 255.255.255.0 area 0 log-adj-changes **redistribute rip subnets** router rip network 192.168.1.0

Vous pouvez voir la table de routage de l'IOS de voisin Router(R2) après avoir redistribué des routes RIP dans l'OSPF AS.

```
R2#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
candidate default, U - per-user static route o - ODR, P - periodic downloaded static route
Gateway of last resort is not set 172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks O
172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1 O 172.16.5.1/32 [110/65] via
172.16.2.2, 01:17:29, Serial1 C 172.16.1.0/24 is directly connected, Ethernet1 C 172.16.2.0/24
is directly connected, Serial1 10.0.0.0/24 is subnetted, 1 subnets C 10.1.1.0 is directly
connected, Ethernet0 O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0 !---
Redistributed route adverstied by Cisco ASA
```

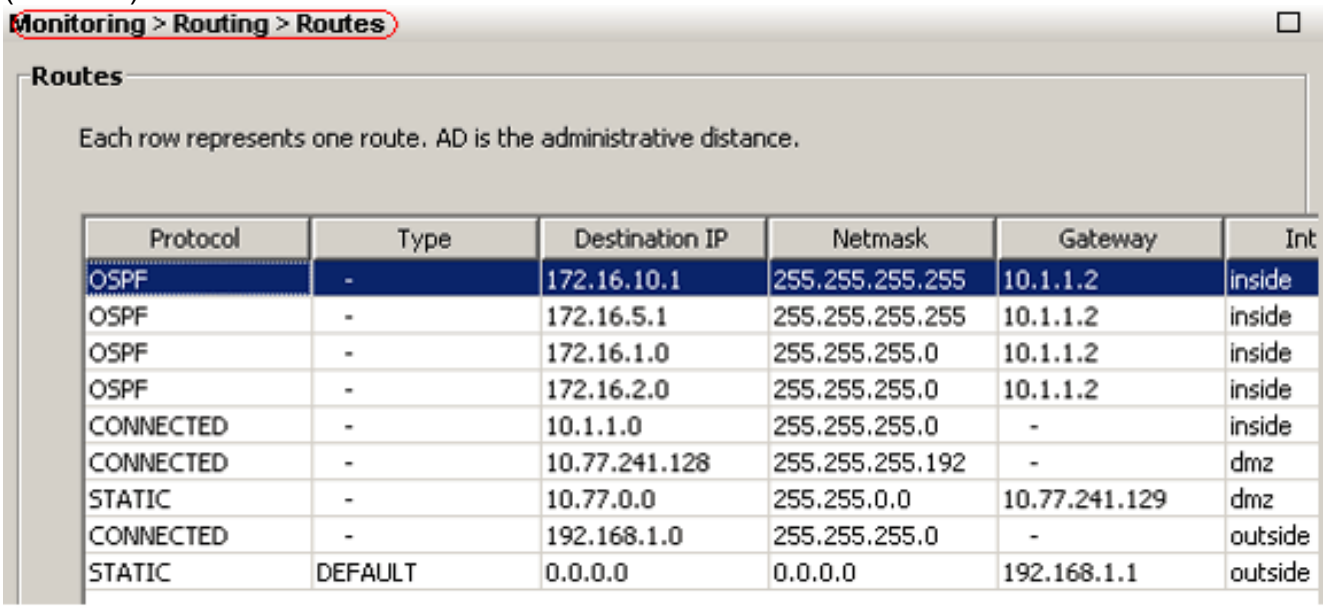
Vérifiez

Terminez-vous ces étapes pour vérifier votre configuration :

1. Sur l'ASDM, vous pouvez naviguer vers la **surveillance > routage > voisins OSPF** pour voir chacun des voisins OSPF. Cette image affiche le routeur interne (R2) en tant que voisin actif. Vous pouvez également voir l'interface où ce voisin réside, l'ID de routeur voisin, l'état, et le temps

d'arrêt.

2. Supplémentaire, vous pouvez vérifier la table de routage si vous naviguez vers la **surveillance > routage > artères**. Dans cette image, les 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24, et 172.16.10.0/24 réseaux sont appris par R2 (10.1.1.2).



3. Du CLI, vous pouvez employer la commande de **show route** afin d'obtenir la même sortie.`ciscoasa#`**`show route`** `Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is 192.168.1.1 to network 0.0.0.0` **`O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside O 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside`** `C 10.1.1.0 255.255.255.0 is directly connected, inside C 10.77.241.128 255.255.255.192 is directly connected, dmz S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz C 192.168.1.0 255.255.255.0 is directly connected, outside S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside`

4. Vous pouvez également employer la commande de **show ospf database** afin d'obtenir des informations sur les réseaux instruits et la topologie OSPF.`ciscoasa#`**`show ospf database`** `OSPF Router with ID (192.168.1.2) (Process ID 1) Router Link States (Area 0) Link ID ADV Router Age Seq# Checksum Link count 172.16.1.2 172.16.1.2 123 0x80000039 0xfd1d 2 172.16.2.1 172.16.2.1 775 0x8000003c 0x9b42 4 172.16.5.1 172.16.5.1 308 0x80000038 0xb91b 3 192.168.1.2 192.168.1.2 1038 0x80000037 0x29d7 1 Net Link States (Area 0) Link ID ADV Router Age Seq# Checksum 10.1.1.1 192.168.1.2 1038 0x80000034 0x72ee 172.16.1.1 172.16.2.1 282 0x80000036 0x9e68`

5. L'ordre de **voisins de show ospf** est également utile afin de vérifier les voisins actifs et les informations correspondantes. Cet exemple affiche les mêmes informations que vous avez obtenues de l'ASDM sur l'étape 1.`ciscoasa#show ospf neighbor Neighbor ID Pri State Dead Time Address Interface 172.16.2.1 1 FULL/BDR 0:00:36 10.1.1.2 inside`

Dépannez

Cette section fournit les informations qui pourraient faciliter dépanner des questions OSPF.

Configuration du voisin statique pour le réseau point par point

Si vous avez configuré la non-*émission point par point de réseau OSPF* sur l'ASA, vous devez définir les voisins statiques OSPF pour annoncer des artères OSPF au-dessus d'un Point à point, réseau de non-diffusion. Référez-vous à définir le pour en savoir plus statique de voisins OSPF.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **mettez au point les événements OSPF** — Active l'élimination des imperfections des événements OSPF.`ciscoasa(config)#debug ospf events OSPF events debugging is on ciscoasa(config)# int e0/1 ciscoasa(config-if)# no shu ciscoasa(config-if)# OSPF: Interface inside going Up OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY OSPF: Backup seen Event before WAIT timer on inside OSPF: DR/BDR election on inside OSPF: Elect BDR 172.16.2.1 OSPF: Elect DR 172.16.2.1 DR: 172.16.2.1 (Id) BDR: 172.16.2.1 (Id) OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abd opt 0x2 flag 0x7 len 32 OSPF: Send with youngest Key 1 OSPF: End of hello processing OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32 mtu 1500 state EXSTART OSPF: First DBD and we are not SLAVE OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152 mt u 1500 state EXSTART OSPF: NBR Negotiation Done. We are the MASTER OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abe opt 0x2 flag 0x3 len 132 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Database request to 172.16.2.1 OSPF: sent LS REQ packet to 10.1.1.2, length 12 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abe opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abf opt 0x2 flag 0x1 len 32 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abf opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE OSPF: Exchange Done with 172.16.2.1 on inside OSPF: Synchronized with 172.16.2.1 on inside, state FULL OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: Neighbor change Event on interface inside OSPF: DR/BDR election on inside OSPF: Elect BDR 192.168.1.2 OSPF: Elect DR 172.16.2.1 OSPF: Elect BDR 192.168.1.2 OSPF: Elect DR 172.16.2.1 DR: 172.16.2.1 (Id) BDR: 192.168.1.2 (Id) OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing` **Remarque:** Référez-vous à la section OSPF de débogage de la référence de commandes d'appareils de sécurité Cisco, version 8.0 pour plus d'informations

sur les diverses commandes qui sont utiles pour dépanner le problème.

Informations connexes

- Page de support pour appliances de sécurité adaptables de la gamme Cisco 5500
- Page de support Cisco 500 gamme PIX
- PIX/ASA 8.X : Configuration d'EIGRP sur le dispositif de sécurité adaptatif dédié (ASA) Cisco
- Support et documentation techniques - Cisco Systems